GENERAL SERVICES ADMINISTRATION
Washington, DC 20405

CIO 2100.1J
December 22, 2015

GSA ORDER

SUBJECT: GSA Information Technology (IT) Security Policy

1. Purpose. This Order issues GSA's Information Technology Security Policy.

2. Cancellations.

a. CIO P 2100.1I CHGE 1, GSA Information Technology (IT) Security Policy is cancelled.

b. CIO IL-14-02 Authority-to-Operate (ATO) Extensions/Limited ATO is cancelled.

c. CIO IL-13-01 Mobile Devices and Applications is cancelled.

d. CIO IL-15-02 Updated Policy Statements for Personally Identifiable Information (PII) is cancelled.

3. Revisions. This Order provides updates for consistency with Federal requirements and program instruction implementation. Changes include:

a. Throughout document, changes were made to support CIO consolidation efforts.

b. Addition of Chapter 6: Privacy Controls.

c. Incorporates information from Instructional Letters: CIO IL-14-02 Authority-to-Operate (ATO) Extensions/Limited ATO, CIO IL-15-02 Updated Policy Statements for Personally Identifiable Information (PII) and CIO IL-14-04 Internal Clearance Process for GSA Data Assets into the policy.

d. Includes information from new Directives: CIO 2130.2 Enterprise IT Governance, CIO 2105.1C CHGE 1 GSA Section 508: Managing Information and Communications Technology (ICT) for Individuals with Disabilities, and MV-15-01 Contract Guidance on Information and Information Systems Security.

e. Includes new public law issued November 2014 – Public Law No: 113-187 Section 10 –Presidential & Federal Records Act Amendments.

f. Incorporates requirements from OAS P 1820.1 GSA Records Management Program.

4. Applicability. This IT Security Policy applies to all individuals or corporate entities that process or handle GSA-owned information, data, all GSA IT systems, or any GSA data processed on IT systems owned and operated by any of the Services or Staff Offices. Contracting Officers must include compliance with this policy in the contract or task order for contractor employees (see Chapter 1 Section 11). This policy applies to the Office of Inspector General (OIG) only to the extent that the OIG determines it is consistent with the OIG's independent authority under the IG Act and it does not conflict with other OIG policies or the OIG mission.

5. Signature.

/S/
DAVID SHIVE
Chief Information Officer
Office of GSA IT

Table of Contents

CHAPTER 1: THE GSA INFORMATION TECHNOLOGY SECURITY PROGRAM

1. Introduction. The purpose of this Order is to document and set forth the General Services Administration (GSA) Information Technology (IT) Security Policy. This IT Security Policy establishes controls required to comply with Federal regulations and laws, thus facilitates adequate protection of GSA IT resources.

2. Objectives. IT Security Policy objectives will enable GSA to meet its mission/business objectives by implementing systems with due consideration of IT-related risks to GSA, its partners, and customers. The security objectives for system resources are to provide assurance of confidentiality, integrity, availability, and accountability, by employing management, operational, and technical security controls as part of risk-based management. An important component of risk-based management is to integrate technical and non-technical security mechanisms into the system to reflect sound risk management practices. All incorporated security mechanisms must be well founded, configured to perform in the most effective manner, and add value to GSA's IT-related investments. A risk-based management approach will enable the GSA IT Security Program to meet its goals by better securing IT systems, enabling management to justify IT Security expenditures, and by assisting management in authorizing IT systems for processing. GSA IT Security objectives include the following:

a. Confidentiality. Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. Private or confidential information is not disclosed to unauthorized individuals while in storage, during processing, or in transit.

b. Integrity. Guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity. Safeguards must ensure that information retains its content integrity. Hardware and software resources of the system must operate according to requirements and design documents. Un-authorized personnel must not be able to create, alter, copy, or delete data processed, stored, or handled by the system. System information and application software is considered "official" and accurate as the basis for business decisions.

c. Availability. Ensuring timely and reliable access to and use of information. The system works promptly and service is not denied to authorized users. Systems and data are available for intended use only. The system must be ready for use by authorized users when needed to perform his/her duties.

d. Accountability. Accountability must be to the individual level. Only personnel with proper authorization and need-to-know must be allowed access to data processed, handled, or stored on IT system components.

e. Assurance. Confidence that the other four security objectives have been met. The security measures, including: technical, managerial, and operational, work as intended to protect the system and the information it processes. This assurance is provided through monitoring and review of controls.

This Order supports GSA's IT Security Program objectives by identifying roles and assigning responsibilities in support of GSA's IT Security Program. In addition, the Order defines comprehensive and integrated security requirements that are necessary to obtain management authorization to allow GSA IT systems to operate within an acceptable level of security risk. The order also supports GSA's objective to ensure that all outsourced cloud services are from FedRAMP compliant cloud service providers, and leverage existing ATOs from other agencies to maximize savings. In addition to the security requirements in this Order, systems that contain payment card data or purchase/credit card numbers must implement the additional security controls known as security requirements as defined in Payment Card Industry Data Security Standard (PCI DSS) published by the PCI Security Standards Council as directed by the Financial Management Services of the Department of Treasury.

3. Federal laws and regulations. The primary focus of this policy is to provide guidelines that support the implementation of the following Federal regulations and laws, and the latest versions of the GSA directives in the next section:

- Federal Information Security Modernization Act (FISMA) of 2014.
- Clinger-Cohen Act of 1996 also known as the Information Technology Management Reform Act (ITMRA) of 1996.
- Federal Financial Management Improvement Act of 1996 (FFMIA); OMB Implementation Guidance for the FFMIA.
- Paperwork Reduction Act (PRA) of 1995 (Public Law 104-13).
- Federal Managers Financial Integrity Act (FMFIA) (Public Law 97-255).
- Government Paperwork Elimination Act (GPEA) (Public Law 105-277).
- Privacy Act of 1974 (5 U.S.C. § 552a).
- Homeland Security Presidential Directive (HSPD-20), National Continuity Policy.
- Homeland Security Presidential Directive (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors.
- Homeland Security Presidential Directive (HSPD-7), Critical Infrastructure Identification, Prioritization, and Protection.
- Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, and Appendix III, Security of Federal Automated Information Systems as amended.
- Public Law No: 113-187, Presidential and Federal Records Act Amendments of 2014, Section10, Disclosure requirement for official business conducted using non-official electronic messaging account.
- Open Data Policy -- Managing Information as an Asset OMB Memorandum M-13-13.
- Payment Card Industry Data Security Standard (PCI DSS)

- Executive Order 13556 Controlled Unclassified Information

4. GSA policies:

- GSA Order ADM 7800.11A, Personal Use of Agency Office Equipment
- GSA Order ADM P 9732.1, Suitability and Personnel Security
- GSA Order CIO 1878.1, GSA Privacy Act Program
- GSA Order CIO 1878.2A, Conducting Privacy Impact Assessments (PIAs) in GSA
- GSA Order CIO 2100.2B, GSA Wireless Local Area Network (LAN) Security
- GSA Order CIO 2102.1, IT Information Technology (IT) Integration Policy
- GSA Order CIO 2104.1A, GSA Information Technology (IT) General Rules of Behavior
- GSA Order CIO 2110.2, GSA Enterprise Architecture Policy
- GSA Order CIO 2135.2B, GSA Information Technology (IT) Capital Planning and Investment Control
- GSA Order CIO 2140.3, Systems Development Life Cycle (SDLC) Policy
- GSA Order CIO 2160.2B, GSA Electronic Messaging and Related Services
- GSA Order CIO 9297.1, GSA Data Release Policy
- GSA Order CIO 9297.2, GSA Information Breach Notification Policy
- GSA Order CIO P 2165.2, GSA Telecommunications Policy
- GSA Order CIO P 2180.1, GSA Rules of Behavior for Handling Personally Identifiable Information (PII)
- GSA Order CIO P 2181.1, Homeland Security Presidential Directive-12 (HSPD-12) Personal Identity Verification and Credentialing
- GSA Order CIO P 2182.2, Mandatory Use of Personal Identity Verification (PIV) Credentials
- Bring Your Own Device: A Toolkit to Support Federal Agencies Implementing Bring Your Own Device (BYOD) Programs, August 23, 2012
- MV-15-01, Contract Guidance on Information and Information Systems Security (GSAM 552.239-71)
- GSA Order CIO IL-15-02, Updated Policy Statements for Personally Identifiable Information (PII)
- GSA Order OAS P 1820.1, GSA Records Management Program

Note:

- In addition to the principles set forth in GSA Order CIO 2110.2, architecture practices cited in OMB's The Common Approach to Federal Enterprise Architecture must be used during planning of a new system or significant capability enhancement.
- Executive Order 13556 implements the Controlled Unclassified Information (CUI) program. OCISO will provide additional guidance upon implementation of the program at GSA. Please contact the OCISO at itsecurity@gsa.gov or the CUI Program Manager at cui@gsa.gov for additional information.

- Additional policies, procedures and guidance can be found in the GSA IT Security InSite main page: https://insite.staging.gsa.gov/portal/category/534722. The guides provide more detailed information on how to implement security processes and controls and provide worksheets and forms to meet reporting requirements. The guides are updated as needed to reflect the latest regulations and technologies. A current list of Government-wide security guidance provided by the National Institute of Standards and Technology (NIST) is located at http://csrc.nist.gov/publications/PubsSPs.html.

5. Compliance and deviation/waivers. Compliance is mandatory immediately upon signing. This IT Security Policy requires all GSA Services, Staff Offices, Regions (S/SO/R), Federal employees, contractors and other authorized users of GSA's IT resources, to comply with the security requirements outlined in this policy. This policy must be properly implemented, enforced, and followed to effectively protect GSA's IT resources and data. Appropriate disciplinary actions must be taken in a timely manner in situations where individuals and/or systems are found non-compliant. Violations of this GSA IT Security Policy may result in penalties under criminal and civil statutes.

All deviations/waivers from this Order must be approved by the appropriate Authorizing Official with a copy of the approval forwarded to the GSA Chief Information Security Officer (CISO) in the Office of GSA IT for concurrence.

6. Maintenance. The GSA Office of the Chief Information Security Officer (OCISO) will review this policy at least annually and revise it to:

- Reflect any changes in Federal laws and regulations;
- Satisfy additional business requirements;
- Encompass new technology;
- Adopt new Government IT standards.

7. Definition of information system. The term *information system* as defined in this document shall include major applications and general support systems as defined in OMB A-130. Major Applications shall include those information systems with an Exhibit 300 (also referred to as Major Programs) and any Exhibit 53 information systems that are not specifically covered in a general support system security plan. In addition, any IT system that stores privacy act data that is not specifically covered in a general support system shall be considered its own information system.

Smaller information systems (minor applications) may be coalesced together as subsystems of a single larger, more comprehensive system for the purposes of security authorization. Subsystems must be under the same management authority, have the same function or mission objective, the same operating characteristics and information security needs, and reside in the same general operating environment(s).

8. National Institute of Standards and Technology (NIST) and GSA guidance documents. All policies shall be implemented using the appropriate special publications

from NIST and/or GSA procedural guides to the greatest extent possible. Where there is a conflict between NIST guidance and GSA guidance, contact the GSA Office of the Chief Information Security Officer. Where there are no procedural guides, use industry best practices. Federal Information Processing Standards (FIPS) publication requirements are mandatory for use at GSA.

NIST special publications (800 Series) are guidance, unless required by a FIPS publication, in which case usage is mandatory. Waivers for compliance to NIST special publications, (refer to 1.6 above for GSA deviations/waivers) must be based on an approved risk based decision that includes a date of resolution to comply.

9. Privacy Act systems. In addition to the security requirements in this Order, systems that contain privacy act data or personally identifiable information must implement the additional security controls as defined in NIST SP 800-53, Appendix J: Privacy Control Catalog, GSA Order CPO 1878.1 Privacy Act Program under “Information Security” and GSA Order CIO 1878.2, CIO P Conducting Privacy Impact Assessments (PIA) in GSA.

10. IT security controls. All IT systems, including those operated by a contractor on behalf of the Government, must implement proper security controls according to the security categorization level in accordance with FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems, FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems, the current version of NIST SP 800-53 R4, Security and Privacy Controls for Federal Information Systems and Organizations.

11. Contractor operations.

a. GSA system program managers and contracting officers shall ensure that the appropriate security requirements of this Order are included in task orders and contracts for all IT systems designed, developed, implemented, and operated by a contractor on behalf of the Government, including systems operating in a Cloud Computing environment including but not limited to Software as a Service (SaaS) and Platform as a Service (PaaS). In addition, the Government shall ensure that the contract allows the Government or its designated representative (i.e. third party contractor) to review, monitor, test, and evaluate the proper implementation, operation, and maintenance of the security controls. This requirement includes, but is not limited to: documentation review, server configuration review, vulnerability scanning, code review, physical data center reviews, and operational process reviews and monitoring of SSAE 16 reporting control submissions.

b. The security controls implemented as part of contracts and task orders must also include specific language that requires solutions to align with existing Information Security architecture. Additional information may be found in IT Security Procedural Guide: Security Language for IT Acquisition Efforts, OCIO-IT Security-09-48.

CHAPTER 2: SECURITY ROLES AND RESPONSIBILITIES

The roles and responsibilities described in the paragraphs below are assigned to the offices and positions identified to ensure effective implementation and management of GSA's IT Security Program. The establishment of a security management structure and assigning of security responsibilities is a requirement of the Federal Information Security Modernization Act (FISMA) of 2014.

1. GSA Administrator. The Clinger-Cohen Act assigns the responsibility for ensuring "that the information security policies, procedures, and practices of the executive agency are adequate." FISMA provides the following details on agency head responsibilities for information security:

a. Providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of an agency, and on information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.

b. Ensuring that an information security program is developed, documented, and implemented to provide security for all systems, networks, and data that support the operations of the organization.

c. Ensuring that information security processes are integrated with strategic and operational planning processes to secure the organization's mission.

d. Ensuring that senior agency officials within the organization are given the necessary authority to secure the operations and assets under their control.

e. Designating a Chief Information Officer (CIO) and delegating authority to that individual to ensure compliance with applicable information security requirements.

f. Ensuring that the agency has trained personnel to support compliance with information security policies, processes, standards, and guidelines.

g. Ensuring that the CIO, in coordination with the other senior agency officials, reports annually to the agency head on the effectiveness of the agency information security program, including the progress of remedial actions.

2. GSA Chief Information Officer (CIO). Mandated by the Clinger-Cohen Act of 1996 and FISMA, the GSA CIO has overall responsibility for the GSA IT Security Program. Responsibilities include:

a. Developing and maintaining an agency-wide GSA IT Security Program.

b. Ensuring the agency effectively implements and maintains information security policies and guidelines.

c. Providing guidance, advice, and assistance to the Heads of Services and Staff Offices (HSSOs), and Regional Administrators (RAs) on implementing GSA's IT Security Policy.

d. Providing management processes to enable the Authorizing Official to implement the components of the IT Security Program for which they are responsible.

e. Ensuring information assurance and the protection of GSA's cyber-based critical infrastructure.

f. Designating a Chief Information Security Officer (CISO) to assist in carrying out the GSA CIO's agency-wide IT security responsibilities.

g. Establishing reporting requirements within GSA to assess GSA's IT security posture, verifying compliance with Federal requirements and approved policies, and identifying agency-wide IT security needs.

h. Conducting independent activities and compliance reviews including oversight of GSA's Assessment and Authorization (A&A) process.

i. Coordinating and reporting on HSPD-7 critical assets.

j. Reporting annually, in coordination with the other senior agency officials, to the GSA Administrator on the effectiveness of the agency information security program, including progress of remedial actions.

k. Reviewing Privacy Impact Assessments prepared by GSA organizations for security considerations.

l. Ensuring Privacy Impact Assessments are part of GSA's System Development Life Cycle Guidance for Information Technology.

m. Providing guidance or input for periodic assessments of S/SO/R security measures and goals to assure implementation of GSA policy and procedures.

3. GSA Chief Financial Officer (CFO). The GSA Chief Financial Officer (CFO) also has major statutory security responsibilities under the CFO Act of 1990 and the Clinger-Cohen Act of 1996. Responsibilities include:

a. Developing and maintaining an integrated agency accounting and financial management system, including financial reporting and internal controls, which comply with FMFIA and FFMIA requirements;

b. Complying with such policies and requirements as may be prescribed by the Director of the Office of Management and Budget (OMB);

c. Complying with applicable accounting principles, standards, and requirements, and internal control standards and any other requirements applicable to such systems;

d. Supporting the GSA IT Capital Planning Process. To achieve satisfactory assurance levels of information security for the financial systems of GSA, close cooperation between the offices of the CFO and the CIO is necessary, including supporting the GSA IT Capital Planning process;

e. Reporting financial management information to OMB as part of the President's budget;

(1) Complying with legislative and OMB-defined responsibilities as they relate to IT capital investments; and

(2) Ensuring that the appropriate security requirements of this Order are included in task orders and contracts for all IT systems designed, developed, implemented, and operated by a contractor that hosts GSA financial systems. This includes, but is not limited to: documentation review of operational processes and reviews that monitor SSAE 16 reporting submissions.

4. GSA Senior Agency Official for Privacy. GSA has identified the CIO as the Senior Agency Official for Privacy (SAOP) having major statutory responsibilities under the Privacy Act of 1974, GSA Order CIO 1878.1, and the Consolidated Appropriations Act of 2005. Responsibilities include:

a. Establishing and overseeing the Privacy Act Program in GSA.

b. Ensuring GSA's compliance with privacy laws, regulations and GSA policy.

c. Ensuring GSA's compliance with NIST SP 800-53, Appendix J: Privacy Control Catalog.

d. Ensuring that GSA data assets go through secure clearance processing prior to public release and that applicable Privacy Policies are followed. The specific policy is detailed in Section 6.7 of this document.

e. Ensuring Privacy Impact Assessments (PIAs) are conducted for electronic information systems and collections and coordinating submission of all GSA Privacy Analysis Worksheets and PIA Summaries to OMB.

f. Developing, implementing, and overseeing personnel security controls for access to personally identifiable information.

g. Encouraging awareness of potential privacy issues and policies.

h. Directing the planning and implementation of the GSA Privacy Program to ensure agency personnel, including contractors, receive appropriate privacy awareness training to include IT Security and Privacy Awareness annual training, Privacy 201 training and Sharing Information in a Collaborative Environment training.

i. Signing GSA Privacy Act notices for publication for public comment in the Federal Register.

j. Reporting to OMB and Congress on the establishment or revision of Privacy Act systems.

k. Reporting periodically to OMB on GSA Privacy Act activities, as required by law and OMB information requests.

l. Policy making role in GSA's development and evaluation of legislative, regulatory and other policy proposals which implicate information privacy issues.

m. Chairing the GSA Data Integrity Board that reviews and approves GSA's Computer Matching Program.

5. GSA Chief Information Security Officer (CISO) (formerly known as Senior Agency Information Security Officer). The Federal Information Security Modernization Act (FISMA) of 2014 establishes the designation of a Senior Agency Information Security Officer. GSA has assigned that responsibility to the Chief Information Security Officer (CISO). The CISO is the focal point for all GSA IT security and must ensure that the security requirements described in this Order are implemented agency-wide. The CISO reports directly to the CIO as required by FISMA Responsibilities include:

a. Reporting to the GSA CIO on the implementation and maintenance of the GSA's IT Security Program and Security Policies.

b. Assisting in the oversight of GSA's IT Security Program and Security Policies.

c. Reporting to the GSA CIO on activities and trends that may affect the security of systems and applications assigned to GSA.

d. Implementing and overseeing GSA's IT Security Program by developing and publishing IT Security Procedural Guides that are consistent with this policy.

e. Ensuring that written agreements assign security-related functions and identify security responsibilities of each S/SO/R or activity when two or more activities use the same IT.

f. Providing guidance and advice to all S/SO/R on IT security issues.

g. Assisting S/SO/R in implementing the IT Security Program and Security Policies when requested.

h. Reporting to agency senior management on policy compliance.

i. Directing the planning and implementation of the GSA IT Security Awareness and Privacy Training Program to ensure agency personnel, including contractors, receive appropriate security and privacy awareness training including “Sharing Information in a Collaborative Environment” training.

j. Managing the CIO Office of the CISO which implements the GSA IT Security and Privacy Programs.

k. Establishing reporting deadlines for IT Security related issues requiring an agency response affecting the GSA IT Security Program.

l. Performing information security duties as the primary duty.

m. Periodically assessing risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency.

n. Periodically testing and evaluating the effectiveness of information security policies, procedures, and practices.

o. Establishing and maintaining a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency.

p. Developing and implementing procedures for detecting, reporting, and responding to security incidents.

q. Ensuring preparation and maintenance of plans and procedures to provide continuity of operations for information systems that support the operations and assets of GSA.

r. Supporting the GSA CIO in annual reporting to the GSA Administrator on the effectiveness of the agency information security program, including progress of remedial actions.

s. Developing and implementing IT security performance metrics to evaluate the effectiveness of technical and nontechnical safeguards used to protect GSA information and information systems.

t. Assessing S/SO/R security measures and goals periodically to assure implementation of GSA policy and procedures.

u. Ensuring the appointment in writing of the ISSM and ISSOs for each system.

v. Administering FISMA requirements and coordinating GSA's annual FISMA security program review and Plan of Action and Milestones (POA&M) implementations.

w. Ensuring that the ISSMs and ISSOs receive applicable security and privacy awareness training to carry out their duties.

x. Ensuring that IT Acquisitions align with GSA Information Security requirements.

6. Heads of Services and Staff Offices (HSSOs). HSSOs are responsible for authorizing the operation of all systems, networks, and applications for which they have responsibility. They may delegate some of their authority, (i.e., the role of Authorizing Official in writing), to appropriately qualified individuals within their organizations. Responsibilities include:

a. Ensuring adherence and proper implementation of GSA's IT Security Policy.

b. Ensuring that the systems of record under their jurisdiction meet the requirements of the Privacy Act and GSA privacy policies and procedures.

c. Ensuring that contractors performing services associated with systems of record (such as system development, maintenance, or operation) are subject to the provisions of the Privacy Act and security requirements.

d. Tracking the measures and goals described in Chapter 3 (i) Performance Measures of this policy and ensuring that AOs, ISSMs, and ISSOs support these measures.

e. Ensuring System Owners adhere to the GSA Records Management Program.

7. Authorizing Official (AO). The Authorizing Official (AO) is the Federal Government management official with the responsibility to identify the level of acceptable risk for an IT system or application and to determine whether the acceptable level of risk has been obtained. Final authority to operate or not operate the system rests with the AO. An AO must be assigned to every information system. An AO may have responsibility for more than one system, provided there is no conflict. Responsibilities include:

a. Ensuring adherence to GSA's IT Security Policy.

b. Reviewing and approving security safeguards of information systems and issuing accreditation statements for each information system under their jurisdiction based on the acceptability of the security safeguards of the system (risk-management approach).

c. Ensuring that an Interim Authorization to Operate (IATO) is granted only if the necessary security enhancements to bring the system to the acceptable level of risk have been identified and a formal plan of action and milestones has been developed. Information systems with an expiring ATO may perform a one-time extension of the current authorization for a period not to exceed one year (365 days) from the date of ATO expiry to allow development of near real-time continuous monitoring capabilities to support ongoing authorization.

d. Ensuring that GSA systems that are planned to be decommissioned may request a one-time ATO extension for a period not to exceed one year (365 days) from the date of the ATO expiry.

e. Ensuring that GSA information systems that are planned to be consolidated into another system or transitioned into a cloud environment may request an ATO extension, for a period not to exceed one year (365 days), to allow the information system to receive an ATO as part of the consolidated information system or its new cloud environment of operation. The scope of consolidation and/or the change in the system environment shall be approved by Office of the Chief Information Security Officer (OCISO) prior to submitting the ATO extension request for the system.

f. Ensuring that GSA information systems that have undergone a full security assessment of all NIST SP 800-53 controls at the appropriate FIPS 199 impact level as part of a three-year re-authorization, and have outstanding high and critical vulnerabilities identified as part of security assessment, may request a limited ATO extension for a period not to exceed 30 days from the date of the ATO expiry to allow mitigation of the high and critical vulnerabilities.

g. Ensure that new GSA information systems pursuing an agile development methodology and residing on infrastructures that have a GSA ATO concurred by the OCISO or a FedRAMP ATO may request a limited ATO for the pilot period of the project not to exceed one year (365 days). The limited ATO will be based on a lightweight security assessment and authorization (A&A) process; however, the period of the limited ATO should be used to conduct a full A&A resulting in a new three-year ATO.

h. Ensuring that under any and all circumstances, in which an ATO is issued for less than three years, the GSA system continues to perform monthly Operating System scans (with Root/Administrative privileges), Database scans (DBA privileges) and Web Application scans (authenticated user privileges). All vulnerabilities identified from the scans shall be resolved; tracked in the systems' Plan of Action and Milestones (POA&M); and submitted to the GSA OCISO.

i. Providing support to the Information System Security Manager (ISSM), of record appointed by the CISO.

j. Providing support to the Information Systems Security Officer (ISSO) of record, appointed by the CISO for each information system.

k. Ensuring Information Assurance (IA) is included in management planning, programming budgets, and the IT Capital Planning process.

l. Requiring written notification of point(s) of contacts within other Federal agencies or outside organizations that manage GSA systems.

m. Ensuring that IT systems that handle privacy data meet the privacy and security requirements of the Privacy Act and IT information security laws and regulations. This includes GSA Order CIO 1878.1, GSA Order CIO 1878.2 and NIST SP 800-53

n. Reviewing and approving Privacy Impact Assessments (PIAs) for their organizations.

o. Supporting the security measures and goals described in Chapter 3(i) (Performance Measures) of this policy.

p. Ensuring all incidents involving data breaches which could result in identity theft are coordinated through GSA IT's Office of the Chief Information Security Officer (OCISO) and the GSA Management Incident Response Team (MIRT) using the GSA breach notification plan per OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, IT Security Procedural Guide: Incident Response (IR), CIO-IT Security-01-02 and GSA Order, CIO 9297.2B, GSA Information Breach Notification Policy.

q. Ensuring contingency and continuity of support plans are developed and tested annually in accordance with OMB Circular No. A-130, NIST SP 800-34, Contingency Planning Guide for Information Technology Systems, and IT Security Procedural Guide: Contingency Planning, OCIO-IT Security-06-29.

r. Implementing detailed separation of duties policies for IT systems based on the specific processes, roles, permissions, and responsibilities of personnel involved in GSA business operations.

s. Establishing physical and logical access controls to enforce separation of duties policy and alignment with organizational and individual job responsibilities.

t. Ensuring access to systems by members of the GSA OIG as described in paragraph 16 of this chapter.

u. Establishing appropriate system/organization unique rules of behavior for systems under their authority.

v. Ensuring that IT systems that handle payment card data meet the security requirements of the in Payment Card Industry Data Security Standard.

8. Office of CISO Division Directors. OCISO Directors are the intermediary to the Authorizing Official for ensuring that security is implemented. The Director is the focal point for all IT system security matters for the IT resources under their responsibility. OCISO Directors report to the CISO. Responsibilities include:

a. Monitoring adherence and proper implementation of GSA's IT Security Policy and reporting the results to the CISO.

b. Reviewing and approving system assessments, prior to forwarding them to the Authorizing Official for approval and the CISO for concurrence.

c. Reviewing and approving assessment and authorization documents to be signed by the appropriate business line representatives and concurred by the appropriate OCISO personnel.

d. Ensuring the security measures and goals described in Chapter 3(i) Performance Measures of this policy are met by the organizations under their responsibility.

e. Ensuring GSA security and privacy awareness training requirements for individuals under their responsibility are complied with.

f. Creating security policies that achieve compliance to appropriately address new security requirements.

g. Advises individuals with IT Security responsibility on proper system security, security "Best Practices" and applicable laws and regulations.

9. Information Systems Security Manager (ISSM). The Information Systems Security Manager (ISSM) is the intermediary to the System Owner and the OCISO Director responsible for ISSO services. There is at least one ISSM per Authorizing Official. The ISSM reports to the OCISO Director for the systems under their authority. An individual appointed as ISSM for a system cannot also be assigned as the ISSO for the same system. Current listings of FISMA Contacts are located on InSite. Responsibilities include:

a. Ensuring adherence and proper implementation of GSA's IT Security Policy.

b. Providing guidance to the ISSOs.

c. Verifying annually the list of ISSOs and providing an updated designation letter to the Director for submission to the CISO when changes occur or designations expire.

d. Ensuring assessment and authorization support documentation is developed and maintained.

e. Reviewing and coordinating reporting of Security Advisory Alerts (SAA), compliance reviews, security and privacy awareness training, incident reports, contingency plan testing, and other IT security program elements.

f. Managing system assessments (including A&A package requirements **PCI DSS Report on Compliance (for IT systems that handle payment card data)**),and forwarding them to the Authorizing Official and OCISO Directors.

g. Forwarding to the appropriate OCISO Director, copies of assessment and authorization documents to be signed by the appropriate individuals as required in A&A guidance.

h. Supporting the security measures and goals described in Chapter 3(i) Performance Measures of this policy.

i. Complying with GSA security and privacy awareness training requirements for individuals with significant security responsibilities.

10. Information Systems Security Officer (ISSO). The Information Systems Security Officer (ISSO) is the focal point for ensuring implementation of adequate system security in order to prevent, detect, and recover from security breaches. An ISSO must be assigned for every information system. An ISSO may have responsibility for more than one system, provided there is no conflict. An individual assigned as the ISSO cannot also be the ISSM for the same system. The ISSO must be knowledgeable of the information and processes supported by the system. The ISSO shall maintain accurate system inventories for information systems for which they have responsibility. A current list of ISSOs is located on InSite at: https://ea.gsa.gov/EAWEB/#!/FISMA_POC. Regional ISSOs (RISSOs) have the same responsibilities as designated ISSOs. Responsibilities include:

a. Ensuring effective implementation of GSA's IT Security Policy.

b. Ensuring the system is operated, used, maintained, and disposed of in accordance with documented security policies and procedures. Necessary security controls should be in place and operating as intended.

c. Advising System Owners of risks to their systems and obtaining assistance from the ISSM, if necessary, in assessing risk.

d. Assisting System Owners in completing and maintaining the appropriate security documentation including the system security plan.

e. Assisting the Authorizing Official in the system assessment and authorization (processes) and creating and maintaining authorization documentation. The ISSO will assist the System Owner to develop and update the system security plan, manage and control changes to the system, and assess the security impact of those changes.

f. Assisting the Authorizing Official, Data Owner and Contracting Officer / Contracting Officer Technical Representative in ensuring users have the required background investigations, the required authorization and need-to-know, and are familiar with internal security practices before access is granted to the system.

g. Promoting information security awareness.

h. Identifying, reporting and responding to security incidents.

i. Reviewing and responding as appropriate to Security Advisory Alerts on vulnerabilities.

j. Ensuring the user identification and authentication scheme used in the system is administered as intended.

k. Ensuring media handling procedures are followed.

l. Reviewing system security audit trails and system security documentation to ensure security measures are implemented effectively.

m. Evaluating known vulnerabilities to ascertain if additional safeguards are needed; ensuring systems are patched, and security hardened.

n. Beginning protective or corrective measures if a security breach occurs.

o. Assisting in the development and maintenance of contingency plan and contingency plan test report documentation.

p. Supporting the security measures and goals described in Chapter 3(i) Performance Measures of this policy.

q. Complying with GSA security and privacy awareness training requirements for individuals with significant security responsibilities.

r. Ensuring Privacy Impact Assessments (PIAs) are completed for IT systems that are new, under development, or undergoing major modifications which impact Privacy Act data.

s. Working with the ISSM and System Owners to develop, implement, and manage POA&Ms for assigned systems IAW IT Security Procedural Guide: Plan of Action and Milestones (POA&M), OCIO-IT Security-09-44.

t. Reviewing system role assignments to validate compliance with principles of least privilege.

u. Assisting the Authorizing Official in PCI DSS Implementation and certification for IT systems that handle payment card data, to include creating and maintaining PCI DSS documentation, and facilitating the self-assessment.

11. System Owners. System Owners (e.g. System Program Managers/Project Managers) are management officials within GSA who bear the responsibility for the acquisition, development, maintenance, implementation, and operation of GSA's IT systems. System Owners represent the interests of the system throughout its lifecycle. Primary responsibility for managing risk and privacy should rest with the System Owners. Responsibilities include:

a. Ensuring effective implementation of GSA's IT Security Policy.

b. Ensuring their systems and the data each system processes have necessary security controls in place and are operating as intended and protected IAW GSA regulations and any additional guidelines established by the OCISO and relayed by the ISSO or ISSM.

c. Obtaining the security resources for their respective systems.

d. Developing and implementing a configuration management plan for their respective systems.

e. Using the advice of the ISSM and ISSO along with the approval of the Authorizing Official, selecting the mix of controls, technologies, and procedures that best fit the risk profile of the system.

f. Participating in activities related to the assessment and authorization of the system to include security planning, risk assessments, security and incident response testing, and contingency planning and testing.

g. Defining and scheduling software patches.

h. Ensuring IT security and privacy requirements are included in IT contracts or contracts including IT.

i. Ensuring implementation of privacy requirements for their system of record.

j. Conducting PIAs on all systems to ascertain whether the system collects information on individuals or when new systems are developed, acquired, or purchased.

k. Developing, implementing and maintaining an approved IT Contingency Plan which includes an acceptable Business Impact Analysis (BIA).

l. Ensuring that information and system categorization has been established for their systems and data IAW FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems.

m. Conducting annual reviews and validations of system users' accounts to ensure the continued need for access to a system and verify users' authorizations (rights/privileges).

n. Ensuring that for each information system, security is planned, documented, and integrated into the system development life cycle (SDLC) from the information system's initiation phase to the system's disposal phase.

o. Reviewing the security controls for their systems and networks annually as part of the FISMA review, when significant changes are made to the system and network and at least every three years or via continuous monitoring based on continuous monitoring plans reviewed and accepted by the GSA CISO.

p. Defining, implementing, and enforcing detailed separation of duties by ensuring that single individuals do not have control of the entirety of a critical process, roles, permissions, and/or responsibilities.

q. Ensuring that physical or environmental security requirements are implemented for facilities and equipment used for processing, transmitting, or storing sensitive information based on the level of risk.

r. Obtaining a written Authorization To Operate (ATO) following GSA Assessment and Authorization processes prior to making production systems operational and/or Internet accessible. Developing and maintaining the system security plan and ensuring that the system is deployed and operated according to the agreed-upon security requirements.

t. Ensuring that system users and support personnel receive the requisite security and privacy awareness training (e.g., instruction in rules of behavior) and assisting in the identification, implementation, and assessment of the common security controls.

u. Supporting the security measures and goals described in Chapter 3(i) Performance Measures of this policy.

v. Complying with GSA security and privacy awareness training requirements for individuals with significant security responsibilities.

w. Integrating and explicitly identifying security funding for information systems and programs into IT investment and budgeting plans.

x. Working with program officials and the system developer on the system's privacy issues, preparing a PIA report, obtaining the Program Manager's approval of the PIA report, and submitting the PIA report to the GSA Personnel Security Officer and GSA IT officials for review and approval.

y. Coordinating with IT security personnel including the ISSM and ISSO and Data Owners to ensure implementation of system and data security requirements.

z. Working with the ISSO and ISSM to develop, implement, and manage POA&Ms for their respective systems IAW IT Security Procedural Guide: Plan of Action and Milestones (POA&M), OCIO-IT Security-09-44.

aa. Ensuring proper separation of duties for GSA IT system maintenance, management, and development processes.

bb. Conducting annual assessments to review the effectiveness of control techniques, with an emphasis on activities that cannot be controlled through logical, physical, or compensating controls.

cc. Working with the Data Owner, granting access to the information system based on a valid need-to-know/need-to-share that is determined during the account authorization process and the intended system usage.

dd. Working with Data Owners with assistance from the ISSO, will ensure system access is restricted to authorized users that have completed required background investigations, are familiar with internal security practices, and have completed requisite security and privacy awareness training programs, such as the annual IT Security & Privacy Act training curriculum.

ee. Working with Data Owners to ensure the appropriate level of auditing and logging data is enabled and generated to support monitoring activities.

ff. Working with Data Owners to ensure that log data is archived for a period of not less than 180 days.

gg. Working with Data Owners to audit user activity for indications of fraud, misconduct, or other irregularities.

hh. Working with Data Owners to document all phases of monitoring activity including monitoring procedures, response processes, and steps performed when reviewing user activity.

ii. Working with the GSA Senior Agency Official for Privacy and Privacy Officer and legal counsel to determine the authority of any program or activity to collect PII.

jj. Reviewing the security controls for its Payment Card systems and networks annually as part of the PCI DSS assessment, when significant changes are made to the system and network.

kk. Working with the Office of the Chief Information Security Officer and Data Owners to respond to any information security incidents that impact the system or the data stored within the system.

ll. Ensuring the GSA Records Management Program is adequately implemented.

12. Data Owners. The Data Owner/Functional Business Line Manager owns the information but not the system application or platform on which the information is processed. Responsibilities include:

a. Determining the security categorization of systems based upon the FIPS Publication 199 levels and ensuring that System Owners are aware of the sensitivity of data to be handled.

b. Coordinating with System Owners, ISSMs, ISSOs, and Custodians to ensure the data is properly stored, maintained, and protected IAW GSA policies, regulations and any additional guidelines established by GSA.

c. Working with the System Owner, with assistance from the ISSO, to ensure system access is restricted to authorized users that have completed required background investigations, are familiar with internal security practices, and have completed requisite security and privacy awareness training programs (such as the annual IT Security & Privacy Act and Sharing Information in a Collaborative Environment training curriculum).

d. Reviewing access authorization listings and determining whether they remain appropriate at least annually.

e. Ensuring protection of GSA's systems and data IAW GSA's IT Security Policy and the GSA Records Management Program.

f. Ensuring that data is not processed on a system with security controls that are not commensurate with the sensitivity of the data.

g. Assisting in identifying and assessing the common security controls where the information resides.

h. Ensuring information systems that allow authentication of users for the purpose of conducting Government business electronically (accessed via the Internet or via other external non-agency controlled networks, such as partner Virtual Private Networks (VPN)) complete an e-authentication risk assessment resulting in an authentication assurance level classification IAW OMB Memorandum M-04-04, E-Authentication Guidance for Federal Agencies.

i. Coordinating with IT security personnel including the ISSM and ISSO and System Owners to ensure implementation of system and data security requirements.

j. Working with the System Owner to ensure the appropriate level of auditing and logging data is enabled and generated to support monitoring activities.

k. Working with the System Owner to ensure that log data is archived for a period of not less than 180 days.

l. Working with the System Owner to audit user activity for indications of fraud, misconduct, or other irregularities.

m. Working with the System Owner to document all phases of monitoring activity including monitoring procedures, response processes, and steps performed when reviewing user activity.

o. Identifying the data assets to catalog in GSA's Enterprise Data Inventory (EDI) and for possible public release.

p. Working with the Office of the Chief Information Security Officer and System Owners to respond to any information security incidents that impact the system or the data stored within the system.

13. Contracting Officers (CO)/Contracting Officer's Representative (COR). The Acquisitions/Contracting Officer function is responsible for managing contracts and overseeing their implementation. For additional information refer to GSAM 539-7002 clauses 552.239 and 552.239-71. Personnel executing this function have the following responsibilities in regards to information security:

a. Collaborating with the CISO or other appropriate official to ensure that the agency's contracting policies adequately address the agency's information security requirements.

b. Coordinating with the CISO or other appropriate official as required ensuring that all agency contracts and procurements are compliant with the agency's information security policy.

c. Ensuring that all personnel with responsibilities in the agency's procurement process are properly trained in information security.

d. Working with the CISO to facilitate the monitoring of contract performance for compliance with the agency's information security policy.

e. Identifying and initiating contractor background investigations in collaboration with the GSA Personnel Security Officer.

f. Ensuring contracts and task orders for ISSM and ISSO services include performance requirements that can be measured.

g. Ensuring that all IT acquisitions include the appropriate security requirements in each contract and task order.

h. Ensuring that the appropriate security and privacy contracting language is incorporated in each contract and task order.

i. Maintaining the integrity and quality of the proposal evaluation, negotiation, and source selection processes while ensuring that all terms and conditions of the contract are met.

j. Ensuring new solicitations include the language of OMB Memorandum M-07-18.

k. Ensuring all GSA contracts, Request for Proposals (RFP), and Request for Quotes (RFQ) involving Privacy Act information adhere to the Federal Acquisition Regulations (FAR) Privacy Act provisions (Subparts 24.1) and include the specified contract clauses (Parts 52.224-1 and 52.224-2), as appropriate.

l. Ensuring industry and Government information technology providers use Security Content Automation Protocol (SCAP) validated tools with the United States Government Configuration Baseline (USGCB) Scanner capability to certify their products operate correctly with USGCB configurations and do not alter USGCB settings.

m. Ensuring new solicitations for all GSA IT systems includes the security contract language from IT Security Procedural Guide: Security Language for IT Acquisition Efforts, OCIO-IT Security-09-48.

14. Custodians. Custodians own the hardware platforms and equipment on which the data is processed. They are the individuals in physical or logical possession of information from Data Owners. Responsibilities include:

a. Coordinating with Data Owners and System Owners to ensure the data is properly stored, maintained, and protected.

b. Providing and administering general controls such as back-up and recovery systems consistent with the policies and standards issued by the Data Owner.

c. Establishing, monitoring, and operating information systems in a manner consistent with GSA policies and standards as relayed by the Authorizing Official.

d. Accessing data only on a need to know basis as determined by the Data Owner.

e. Providing the Office of the Chief Information Security Officer physical access to devices when needed as part of any incident response effort.

15. Authorized users of IT resources. Authorized users of GSA IT resources, including all Federal employees and contractors, either by direct or indirect connections, are responsible for complying with GSA's IT Security Policy. Their responsibilities include:

a. Complying with all GSA security policies and procedures.

b. Complying with security and privacy awareness training, education, and awareness sessions commensurate with their duties.

c. Reporting any observed or suspected security problems/incidents to their local IT Service Desk .

d. Complying with background investigation policies.

e. Familiarizing themselves with any special requirements for accessing, protecting, and using data, including Privacy Act requirements, copyright requirements, and procurement-sensitive data.

f. Ensuring that adequate protection is maintained on their workstation, including not sharing passwords with any other person and logging out, locking, or enabling a password protected screen saver before leaving their workstation.

g. Ensuring Personally Identifiable Information (PII) and/or sensitive data stored on any workstations or mobile devices including, but not limited to, laptop computers, notebook computers, external hard drives, USB drives, CD-ROMs/DVDs, personal digital assistants is encrypted with GSA provided encryption. Employees and contractors may access PII remotely [i.e., remote access is when the individual is not physically located in a GSA facility (e.g., when the individual is teleworking)] unless explicitly prohibited by the GSA Senior Agency Official for Privacy (SAOP) and/or the Authorizing Official (AO) for the particular information system, in coordination with the Data Owner and/or the GSA Supervisor. All access shall only be from Government Furnished Equipment (GFE) or through an approved GSA virtual interface (i.e. Citrix and/or VDI). In addition, an individual shall not download or store PII on non-GFE. Approval to telework is at the discretion of the GSA Supervisor and/or Contracting Officer, as applicable, and in conformance with GSA Order HCO 6040.1A, GSA Mobility and Telework Policy.

h. Ensuring GSA managed computers that collect and store PII must adhere to all PII requirements.

i. Utilizing assigned privileged access rights (power user, database administrator, web site administrator, etc.) to a computer based on need to know.

16. GSA Inspector General (IG). The GSA IG is the focal point for a statutory office within an organization that, in addition to other responsibilities, works to assess an organization's information security practices and identifies vulnerabilities and the possible need to modify security measures. The Office of Inspector General (OIG) completes this task by:

a. Detecting fraud or instances of waste, abuse, or misuse of an organization's funds.

b. Identifying operational deficiencies within the organization.

c. Performing annual independent FISMA evaluations.

d. Accessing GSA and contractor records. OIG auditors, investigators, inspectors, and attorneys must be provided access to all records, reports, reviews, documents, papers, and materials available to GSA and pertaining to agency programs and activities. When performing reviews of contractor records and proposals, access to information is provided by statute, contract terms, and agreements between the contractor and the Government. To facilitate the process of gaining access to information, auditors, investigators, inspectors, and attorneys carry credentials identifying them as OIG officials. In addition, the following procedures will be followed to allow OIG personnel access to GSA electronic systems:

(1) For the OIG, the point of contact will be the Assistant Inspector General for Auditing (AIGA) or his/her designees. For the Services and Staff Offices within GSA, the points of contact will be the Authorizing Official (AO) for each information system.

(2) The AIGA will notify the AO of the electronic system within his or her purview to which OIG personnel need access.

(3) The AO will inform the AIGA what the highest classification level is of information on the system and all security and privacy awareness training that is required of GSA and/or contractor personnel in order to access the system.

(4) The AIGA will designate the OIG personnel who are to be given access and ensure they have appropriate clearance levels.

(5) The AIGA will certify that each OIG person who may have access to the system has completed all security and privacy awareness training required of GSA personnel before access is granted.

(6) The AIGA will annually certify that each OIG person with access to a GSA system has a continuing need for access and has maintained up-to-date training requirements in connection with the System Owner's annual review and validation of systems users' accounts as described in paragraph 2.10 of this chapter.

(7) The AIGA will ensure and state that access is necessary for OIG personnel to accomplish assigned tasks IAW the OIG's organizational mission and functions. The following statement from the AIGA will suffice to establish that access is necessary for these purposes: "This access is requested to fulfill the OIG's statutory responsibility to conduct and supervise audits, inspections, and investigations relating to the programs and operations of GSA, and to promote economy, efficiency and effectiveness in the

administration of, and to prevent and detect fraud, waste, and abuse in GSA programs and operations."

(8) With regard to requests for access to Privacy Act systems of records, the AIGA will ensure and certify that the OIG personnel who will be accessing the system have a need for the records in the performance of their duties. The statement shall suffice to establish that access to the system is consistent with the requirements of the Privacy Act.

(9) The AO will work with the System Owner to ensure access is granted promptly after the above steps have been completed. If access cannot be granted within fourteen (14) calendar days after completion of the above steps, the AO will inform his/her HSSO and the AIGA and will work with the AIGA to resolve any impediments to OIG access to the system. The Chief Information Officer, or designee, will assist as requested in resolving any issues.

(10) The System Owner will authorize OIG personnel to access GSA-owned information systems from the OIG's accredited system. When possible under contractual terms, OIG personnel will be authorized access to contractor-owned information systems from the OIG's accredited system.

(11) To the extent practicable, OIG personnel will not be granted access to other agencies' owned or controlled records or information about other agencies and their employees that may be maintained in a GSA-controlled system, absent the other agency's permission.

(12) The OIG will advise the AO immediately if circumstances change such that access is no longer needed; for example, if an individual with access leaves the OIG, or upon conclusion of the investigation/inspection/audit or other OIG purpose for which systems access was provided.

(13) OIG employees will have "read-only" access to all information in the system. OIG personnel will not be able to add to, delete, or modify the data in the system.

(14) Each OIG employee with access will use a unique identifier and password when accessing the system.

(15) Testing in support of an OIG review, whether manual or automated, shall not have an adverse effect on the operational production status of the IT system being reviewed other than the increase in usage/traffic due to additional users.

(16) OIG operational needs may preclude OIG staff from obtaining the required approvals prior to removal of personally identifiable information from GSA facilities. The following statement from the AIGA will suffice to establish that requirement is necessary for these purposes: "This access is requested to fulfill the OIG's statutory responsibility

to conduct and supervise audits, inspections, and investigations relating to the programs and operations of GSA, and to promote economy, efficiency and effectiveness in the administration of, and to prevent and detect fraud, waste, and abuse in, GSA programs and operations."

(17) Should the system be compromised by a reportable incident, and the access of OIG personnel be implicated in the incident, the System Owner will promptly notify the Inspector General in writing, and the Inspector General will take appropriate action with respect to the employee(s) responsible.

17. GSA Personnel Security Officer/Office of Human Resources Management. The GSA personnel security officer is responsible for the overall implementation and management of personnel security controls across GSA, to include integration with specific information security controls. As information security programs are developed, Chief officials should work to ensure this coordination of complementary controls. In consideration of information security, the personnel security officer has responsibility for:

a. Developing, promulgating, implementing, and monitoring GSA personnel security programs.

b. Developing and implementing position risk designation (including third-party controls), access agreements, and personnel screening, termination, and transfer procedures.

c. Ensuring consistent and appropriate sanctions for personnel violating management, operation, or technical information security controls.

d. There shall be no waivers to background investigations for IT access for GSA employees or contractors. A favorable initial fitness/suitability determination shall be granted before access to the GSA network or any GSA IT system.

18. System/Network administrators. System/Network Administrators are responsible for:

a. Ensuring the appropriate security requirements are implemented consistent with GSA IT security policies and hardening guidelines.

b. Implementing system backups and patching of security vulnerabilities.

c. Utilizing privileged access rights (e.g., "administrator," "root," etc.) to a computer based on a need to know.

d. Working with the Custodian/ISSO to ensure appropriate technical security requirements are implemented.

e. Ensuring System/Network administrators have separate Administrator and User accounts, if applicable (e.g., Microsoft Windows accounts). The Administrator privileged account must only be used when Administrator rights are required to perform a job function. A normal user account should be used at all other times.

f. Identifying and reporting security incidents and assisting the OCISO, in resolving the security incident.

g. Utilizing GSA provided Multifactor Authentication is being used to ensure strong authentication.

19. Supervisors. Supervisors are responsible for:

a. Conducting annual review and validation of staff user accounts to ensure the continued need for access to a system.

b. Conducting annual reviews of staff training records to ensure annual IT Security Awareness, Privacy Act, Security Training, and application specific training was completed for all users. The records shall be forwarded to application ISSO/System Owners as part of the annual recertification efforts.

c. Coordinating and arranging system access requests for all new or transferring employees and for verifying an individual's need-to-know (authorization).

d. Coordinating and arranging system access termination for all departing or resigning personnel.

e. Coordinating and arranging system access modifications for personnel.

f. Documenting job descriptions and roles to accurately reflect the assigned duties, responsibilities, and separation of duties principles. Establishing formal procedures to guide personnel in performing their duties, with identification of prohibited actions.

CHAPTER 3: POLICY ON MANAGEMENT CONTROLS

This chapter provides the basic management control security policy statements for GSA systems. Management Controls deal with the overall control of the security program for GSA, including networks and systems. The policy statements are derived primarily from OMB Circular A-130 and are integral to an effective IT security program. The manner in which these controls are implemented depends on the risks, sensitivity, and criticality associated with the specific systems and data involved. In some cases, basic security policy controls may need to be modified or supplemented in order to address application-specific or system-specific requirements.

1. According to NIST, the Management Controls are obtained from the following Control Families:

- Certification, Accreditation, and Security Assessments (CA)
- Planning (PL)
- Program Management (PM)
- Risk Assessment (RA)
- System and Services Acquisition (SA)

2. The following paragraphs provide specific policy on controls for the security management of GSA systems.

a. Assign responsibility for security.

(1) A security management structure must be established and security responsibilities must be clearly assigned.

(2) Responsibility for the security of the IT system must be assigned to an Authorizing Official.

(3) Responsibility for ensuring security is implemented across the Services, Staff Offices, or Regions must be assigned, in writing, to an ISSM.

(4) Responsibility for each major application and general support system within the Services, Staff Offices or Regions must be assigned, in writing, to an ISSO.

b. Risk management.

(1) Authorizing Officials must implement a risk management process for all information systems using NIST SP 800-30: Guide for Conducting Risk Assessments and GSA IT Security 06-30: Managing Enterprise Risk – Security Assessment and Authorization, Planning and Risk Assessment and all identified A&A process procedural guides as required.

(2) Authorizing Officials must ensure risk assessments are performed and documented as part of assessment and authorization activities before a system is placed into production, when significant changes are made to the system and at least every three (3) years or via continuous monitoring based on GSA CIO IT Security 12-66: Continuous Monitoring Program that is reviewed and accepted by the GSA CISO.

(3) All information systems must use NIST SP 800-60: Guide for Mapping Types of Information and Information Systems to Security Categories and FIPS Publication 199 Standards for Security Categorization of Federal Information and Information Systems to determine their security category (i.e. risk level) for confidentiality, availability and integrity.

(4) All information systems that allow authentication of users for the purpose of conducting government business electronically (accessed via the Internet or via other external non-agency controlled networks, such as partner VPN) complete an e-authentication risk assessment resulting in an authentication assurance level classification IAW OMB Memorandum M-04-04, E-Authentication Guidance for Federal Agencies.

(5) Authorizing Officials must ensure that the risk management process includes contingency and continuity of support plans developed and tested annually IAW Office of Management and Budget (OMB) Circular No. A-130, NIST SP 800-34, Contingency Planning Guide for Information Technology Systems, and GSA CIO-IT-Security 06-29: IT Security Procedural Guide: Contingency Planning.

(6) All information systems must develop and maintain Plan of Action and Milestones (POA&M) in accordance with IT Security Procedural Guide: Plan of Action and Milestones (POA&M), OCIO-IT Security-09-44. POA&Ms are the authoritative agency management tool for managing system risk and used in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in agency programs and systems. GSA must submit POA&Ms to OMB upon request.

(7) All FIPS 199 Low impact and Moderate impact Internet accessible information systems, and all FIPS 199 High impact information systems are required to complete an independent penetration test (or 'pentest') and provide an Independent Penetration Test Report documenting the results of the exercise as part of the Assessment and Authorization (A&A) package. NIST 800-53 R3 control CA-2(2) and NIST 800-53 R4 control CA-8 requires FIPS 199 High impact systems to complete penetration tests annually. The annual penetration tests can be completed internally and do not require an independent assessor. In addition, all Internet facing systems in the GSA CIO IT Security 12-66: Continuous Monitoring Program must conduct penetration testing annually. In addition, all systems undergoing the Lightweight ATO process must conduct penetration testing.

c. Review of security controls.

(1) Every IT system both government and contractor operated must undergo a security control assessment utilizing the current version of NIST SP 800-53Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans, and the annual requirements provided by the OCISO.

(2) The OCISO must submit, on behalf of the CIO, an agency-wide FISMA Report to OMB and specified congressional committees annually.

(3) An entity-wide IT security program must include compliance reviews to determine how well the over-all GSA security program meets the agency performance measures.

d. Lifecycle.

(1) GSA IT Security Policy must be incorporated into each phase of the lifecycle, (i.e., initiation, development/acquisition, implementation, operation and disposal) for all GSA information systems.

(2) System owners must use NIST SP 800-64 Security Considerations in the Information System Development Life Cycle, GSA Order CIO P 2140.3, Systems Development Life Cycle (SDLC) Policy, and the GSA Solutions Life Cycle Handbook as guides when managing security throughout the system's lifecycle.

(3) The Security Engineering Division (ISE) in the OCISO must participate in the Executive Business Case review process as a member of the Enterprise Architecture Review Board (EARB)

(4) The ISE must approve all contract documents, such as RFPs and SOWs prior to publication,

(5) The ISE must approve all Security Architecture designs prior to implementation.

e. Authorized processing.

(1) The AO must authorize, in writing, all information systems before they go into operation.

(2) All GSA information systems must be assessed and authorized at least every three (3) years or whenever there is a significant change to the system's security posture IAW NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, and IT Security Procedural Guide: Managing Enterprise Risk, OCIO-IT Security-06-30.

(3) As part of the assessment and authorization process, all systems must be categorized in accordance with FIPS PUB 199, and NIST SP 800-60. Risk Assessments must be performed IAW NIST SP 800-30. E-authentication risk assessments must be performed IAW OMB M-04-04. All controls must be implemented IAW FIPS PUB 200 and the current version of NIST SP 800-53. All controls must be documented in the system's security plan IAW NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems. All controls must be documented and tested IAW NIST SP 800-53A, Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans and any other supplemental GSA guidance. In addition, contingency plans must be developed IAW NIST SP 800-34 and have been tested IAW GSA-CIO-IT Security 06-29 within the past year in order for the Authorizing Official to authorize the system to operate (i.e. accredit).

(4) A Lightweight ATO (aka Limited ATO) can be issued to a Low or Moderate impact system for an initial ninety (90) day period based on the results of a Pen Test. This can be extended up to a year for Moderate or a full three year ATO for low impact systems in the GSAIT organization, pursuing an agile development methodology AND residing on infrastructures that have a GSA ATO concurred by the GSA CISO or a FedRAMP ATO.

(5) Information systems with expiring Authorizations to Operate (ATO) may request a one-time extension of the current authorization for a period not to exceed one year from the date of ATO expiration if during this time the system will be decommissioned or to allow development of near real-time continuous monitoring capabilities to support ongoing authorization. ATO extensions must be supported by current vulnerability assessment results (operating system, database, and web (as applicable)) and POA&M identifying weaknesses from all sources. AOs must obtain approval from the CISO for the continuous monitoring plans of systems authorizations that have been extended. Plans must be approved within 6 months of the extension. New systems and systems that have undergone or are undergoing a significant change must adhere to the current GSA Risk Management Framework processes as documented in GSA CIO-IT Security-06-30.

(6) All GSA information systems must complete a Privacy Impact Assessment (PIA) as part of the assessment and authorization process. The PIA must be reviewed and updated annually or more frequently if there is a significant change to the system's privacy posture.

(7) Private sector cloud computing Software as a Service (SaaS) solutions that are implemented for limited duration and/or one time use; involve data already in the public domain or data that is non-sensitive and could be considered minimal impact; GSA would not be harmed regardless of the consequence of an attack or compromise, and the dollar cost for such a deployment does not exceed $100,000 annually, may follow the streamlined assessment and authorization approach defined in IT Security Procedural Guide: Managing Enterprise Risk, OCIO-IT Security-06-30, for such

systems. AOs must consider Federal and agency information security requirements, and the S/SO security needs. An evaluation of the data and project scope must be performed to assure the conditions noted above are met. A review of the security controls and activities for such systems must be performed to assure the security controls and practices of the contractor are adequate before authorizing use and accepting residual risk.

f. System Security Plan (SSP).

(1) All information systems must be covered by a security plan IAW the current version of NIST SP 800-18.

(2) Update SSPs at least annually or when significant changes occur to the system.

g. Rules of the system.

(1) Authorized users must be provided written Rules of Behavior IAW GSA Order CIO 2104.1 before being allowed access into any GSA, non-public information system.

(2) The user must acknowledge receipt of these rules through a positive action.

h. System interconnections/information sharing.

(1) Written management authorization for system interconnection, based upon the acceptance of risk to the IT system, must be obtained from the AOs of both systems prior to connecting a system not under a single AO's control IAW NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems. Per NIST 800-47, an interconnection is the direct connection of two or more IT systems for the purpose of sharing data and other information resources through a pipe, such as ISDN, T1, T3, DS3, VPN, etc.

(2) If GSA systems interconnect, they must connect using a secure methodology that provides security commensurate with the acceptable level of risk as defined in the system security plan and that limits access only to the information needed by the other system.

(3) All interconnections between GSA and external entities including off-site contractors or Federal agency/departments must be approved by the AO and concurred by the GSA CISO, and reviewed on an annual basis, at a minimum.

i. Performance measures. HSSOs, for their FISMA reportable systems, shall track the measures / goals presented by the CISO. AOs, System Owners, ISSMs, and ISSOs shall support these measures. The CISO shall periodically assess and report on the performance and goals.

j. Plan of Action and Milestones (POAMs). Capture all information security program and system weaknesses that require mitigation in the POA&M IAW GSA CIO-IT Security-09-44. POA&Ms shall be updated quarterly.

k. Contractors and outsourced operations. Implement appropriate safeguards to protect GSA information and information systems from un-authorized access throughout all phases of a contract. Review contracts to ensure that information security is appropriately addressed in the contracting language. GSA CIO-IT Security 09-48 establishes the security language for GSA IT acquisitions contracts involving contractors. All applicable NIST 800-53 controls should be put on contract (and a reasonable subset continuously monitored using guidance provided by the OCISO) for all contractor and outsourced operations. Given that the GSA IT security program is risk-based, it may not always make financial sense to mandate all NIST 800-53 IT security controls on an outsourced system. The System Program Manager and ISSO should make risk-based decisions on which controls could potentially be waived and then obtain concurrence from the Authorizing Official and the CISO.

l. Privacy Impact Assessments (PIAs). Conduct PIAs on all GSA information systems IAW OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 that includes, but is not limited to, the collection of new information in identifiable form (IIF). IFF is information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, e-mail address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors, aka PII or when new information systems are developed, acquired, and/or purchased. The PIA must be reviewed and updated annually or more frequently if there is a significant change to the system's privacy posture IAW GSA Order CPO 1878.1 GSA Privacy Act Program.

m. Capital planning and investment. Integrate and explicitly identify funding for information systems and programs into IT investment and budgeting plans per NIST Special Publication 800-65: Integrating IT Security into the Capital Planning and Investment Control Process and GSA Order CIO 2135.2, GSA Information Technology (IT) Capital Planning and Investment Control. GSA’s capital planning and investment control process must be used for the continuous selection, control, and evaluation of IT investments over their life cycles.

n. Enterprise Architecture (EA). Systems shall be implemented per the enterprise architecture principles in CIO 2110.2 GSA Enterprise Architecture Policy. The principles contained in GSA Order CIO 2110.2 are consistent with OMB Circular A-130 which establishes the framework for architecture to address security controls for components, applications, and systems.

(1) In addition to the principles set forth in GSA Order CIO 2110.2, architecture practices cited in OMB's Federal Segment Architecture Methodology must be used during planning a new system or significant capability enhancement.

(2) GSA OCISO has determined that the implementation of enterprise architecture principles is provided as a common control by the Office of Enterprise Planning and Governance (IE). For additional details, please refer to the GSA Information Security Program Plan.

CHAPTER 4: POLICY ON OPERATIONAL CONTROLS

This chapter provides the basic operational control security policy statements for GSA systems. Operational Controls concern requirements to design, maintain, and use GSA systems in a secure environment. The policy statements are derived primarily from OMB Circular A-130 and are integral to an effective IT security program. The manner in which these controls are implemented depends on the risks, sensitivity, and criticality associated with the specific systems and data involved. In some cases, basic security policy controls may need to be modified or supplemented in order to address application-specific or system-specific requirements.

1. According to NIST, the Operational Controls are obtained from the following Control Families:

- Awareness and Training (AT)
- Configuration Management (CM)
- Contingency Planning (CP)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Physical and Environmental Protection (PE)
- Personnel Security (PS)
- System and Information Integrity (SI)

2. The following paragraphs provide specific policy on controls for the operational security of the system.

a. Personnel security.

(1) Background investigation requirements for access to GSA information systems (including contractor operations containing GSA information) shall comply with GSA Order CIO P 2181.1 GSA HSPD-12. Contractors requiring non-routine access to IT systems (contractor summoned for an emergency service call) are not required to have a personnel investigation and are treated as visitors and must be escorted while in a GSA facility.

(2) Termination and Transfer Procedures must be incorporated into the authorization process for all information systems. Refer to the GSA-CIO-IT Security 03-23: Termination and Transfer Procedural Guide for additional details.

(3) Supervisors of GSA employees and CORs of GSA contractors must be responsible for coordinating and arranging system access requests for all new or transferring employees and for verifying an individual’s need-to-know (authorization).

(4) Supervisors of GSA employees and CORs of GSA contractors must be responsible for coordinating and arranging system access termination for all departing or resigning personnel.

(5) User authorizations must be verified annually for all information systems.

(6) The Authorizing Official or their designee must grant remote access (i.e. external to GSA's network) privileges only to those GSA employees and contractors with a legitimate need for such access as approved.

(7) Employees and contractors shall have a favorable initial fitness/suitability determination and be in the process of receiving a Minimum Background Investigation (or comparable investigation) or higher to access PII. The authority and access shall be determined by the appropriate GSA Supervisor (for GSA employees) or Contracting Officer (for contract personnel), Data Owner, and the System's Authorizing Official (AO). Each System's AO, with the request of the GSA Supervisor, Data Owner or Contracting Officer, shall evaluate the risks associated with each such request. To find Authorizing Officials go to https://ea.gsa.gov/ and click on "Security" then "FISMA Systems – POC."

(8) There shall be no waivers to background investigations for IT access for GSA employees or contractors. A favorable initial fitness/suitability determination shall be granted before access to the GSA network or any GSA IT system.

b. Physical and environmental protections.

(1) Physical and environmental security controls must be commensurate with the level of risk and must be sufficient to safeguard IT resources against possible loss, theft, destruction, accidental damage, hazardous conditions, fire, malicious actions, and natural disasters.

(2) GSA servers, routers, and other communication hardware essential for maintaining the operability of GSA systems and their connectivity to the GSA Network, must be placed in an isolated, controlled-access location (i.e., behind locked doors).

(3) Limit access to rooms, work areas/spaces, and facilities that contain agency systems, networks, and data to authorized personnel. A list of current personnel with authorized access shall be maintained and reviewed annually to verify the need for continued access and authorization credentials.

(4) Visitor access records shall be maintained for facilities containing information systems (except for those areas within the facility officially designated as publicly accessible). Visitor access records include: (i) name and organization of the person visiting; (ii) signature of the visitor; (iii) form of identification; (iv) date of access; (v) time of entry and departure; (vi) purpose of visit; (vii) name and organization of person visited, and (viii) signature and name of individual verifying the visitor's credentials. Visitor access records shall be reviewed at least annually.

(5) Ensure that all agency systems and networks are located in areas not in danger of water damage due to leakage from building plumbing lines, shut-off valves, and other similar equipment to support meeting federal and local building codes.

(6) Install and ensure operability of fire suppression devices, such as fire extinguishers and sprinkler systems, and detection devices, such as smoke and water detectors, in all areas where agency information systems are maintained (this includes server rooms, tape libraries, and data centers) to meet federal and local building codes.

(7) Install and ensure operability of air control devices, such as air-conditioners and humidity controls, in all areas where agency information systems are maintained (this includes server rooms, tape libraries, and data centers) to meet federal and local building codes.

(8) Ensure that guidance provided in the GSA CIO-IT Security – 12-64: Physical and *Environmental Protection* for a secure environment for information systems, including physical access control, fire protection, emergency power, and alternate sites are implemented. Facilities management offices may be heavily involved in implementing these controls, especially where controls are associated with multiple systems.

c. Production and input/output controls. Data (including relevant and pertinent documentation) must be protected against unauthorized access, tampering, alteration, loss, and destruction during production, input, output, handling, and storage. This protection must include clarification for labeling sensitive security documentation IAW GSA policies. Additional guidance may be found in GSA CIO-IT Security-12-63: System and Information Integrity.

d. IT contingency planning/continuity of support planning. Contingency planning focuses on the recovery and restoration of an IT system following a disruption. The contingency plan supports the agency Continuity of Operations Plan (COOP) required by HSPD-20, National Continuity Policy, ensuring that Primary Mission-Essential Functions continue to be performed during a wide range of emergencies. Contingency and continuity of support plans must be developed and tested annually for all IT systems in accordance with OMB Circular No. A-130, NIST SP 800-34, and GSA CIO-IT Security-06-29.

(1) A system specific IT contingency plan must be developed that identifies and addresses preventive controls, damage assessment procedures, plan testing and training procedures.

(a) The Security Engineering Division in the Office of the Chief Information Security Officer must participate in the Executive Business Case review process as a member of the Enterprise Architecture Review Board (EARB)

(b) The Security Engineering Division in the Office of the Chief Information Security Officer must approve of all contract documents, such as RFPs and SOWs prior to publication.

(c) The Security Engineering Division in the Office of the Chief Information Security Officer must approve of all Security Architecture Designs prior to implementation.

(2) Each contingency plan must include an approved BIA recovery strategy and documented procedures to maintain the plan.

(3) Personnel supporting FIPS 199 Low, Moderate and High impact systems with contingency planning responsibilities shall be trained in their contingency roles and responsibilities with respect to the information system annually with refresher training every three years.

(4) The contingency plan must be annually tested IAW GSA CIO-IT Security-06-29.

(5) Continuity of operations plan (COOP) contact lists which only contain a person's name and home phone number are exempt from GSA IT security policy requirements in this policy. COOP contact lists kept on an electronic device that is password protected (other Government approved Smart Phone devices, laptop, USB drive) do not require written permission or encryption. Paper "cascade lists" limited to name and home phone number that are maintained for the purpose of emergency employee accountability are permissible with the approval of those individuals listed. All paper and other media should be kept in a locked facility or an otherwise secure location when not in use.

(6) The contingency plan must be updated annually to address system/organizational changes or problems encountered during plan implementation, execution, or testing.

e. Hardware and software maintenance.

(1) The availability and usability of GSA equipment and software must be maintained and safeguarded to enable agency objectives to be accomplished.

(2) Lost or stolen GSA IT assets must be immediately reported to the IT Service Desk.

(3) All information systems must be securely hardened and patched before being put into operation and while in operation.

(4) Maintenance of agency hardware and software must be restricted to authorized personnel.

(5) Hardware and software must be tested in a non-production environment to identify adverse effects on system functionality, be documented, and approved prior to promotion to production.

(6) In GSA facilities, only approved Government Furnished Equipment (GFE) is allowed connection (e.g., Ethernet) to the network unless specifically approved by the General Support System Authorizing Official. All non-GFE will be given Internet only access, if possible.

(7) All GFE, to include hardware, software and COT applications, must be approved through the GSA Helpdesk approval process prior to procurement.

(8) Ensure that maintenance activities of hardware and software are IAW with GSA-IT-Security 10-50: Maintenance.

f. Data integrity.

(1) Data integrity and validation controls must be used on all information systems that require a high degree of integrity.

(2) All information systems must have up-to-date virus protection software.

(3) Ensure that data integrity is protected IAW GSA CIO-IT Security-12-63: System and Information Integrity.

g. Documentation. Security related documentation must be obtained or created to describe how security mechanisms are implemented and configured within the IT system. This includes but is not limited to:

- System Security Plan
- Configuration Management Plan
- Contingency Plan
- Privacy Impact Assessments

h. Security and privacy awareness, training, and education.

(1) A security and privacy awareness, training and education program must be established by the OCISO to ensure all GSA, other agency, and contractor support staff involved in the management, design, development, operation, and use of IT systems are aware of their responsibilities for safeguarding GSA systems and information.

(2) All GSA employees and contractors (internal and external*) must provide verification that Security Awareness Training and Privacy Training approved by GSA has been completed within 30 days of notification to complete the training and annually thereafter.

(3) All GSA employees and contractors (internal and external*), who have significant information security responsibilities as defined by OPM 5 CFR Part 930 and GSA IT security training policy, must complete specialized IT security training as defined in the policy.

(4) Failure to comply with annual awareness and specialized IT security training requirements will result in termination of access to GSA information systems. Authorizing Officials can terminate system accounts.

(5) Privacy 201 training is for managers, supervisors and employees that receive privacy data in the course of conducting GSA business. All employees and contractors shall complete “IT Security Awareness and Privacy 101 Training,” “Privacy Training 201,” and the “Sharing in a Collaborative Environment” training before being provided access to any PII, as defined in OMB Memorandum M-07-16 and M-10-23.

* An external contractor is defined as someone who has access to GSA information but doesn't have a GSA e-mail account.

i. Incident response capability.

(1) Every S/SO/R must establish a security incident response capability for detecting, reporting, and responding to security incidents.

(2) All authorized IT users must be trained annually to promptly report suspected vulnerabilities, security violations, and security incidents to their IT Service Desk. Refer to GSA-CIO-IT Security 01-02 for additional details.

(3) ISSOs must report security incidents through the IT Service Desk to the CISO IAW GSA CIO-IT Security-01-02. The OCISO shall then report incidents to the GSA Office of Inspector General IAW that Procedural Guide.

(4) All incidents involving the loss or theft of GSA hardware, software, and/or information in physical form, occurring in GSA Federal facilities, must be reported to the GSA OIG. The GSA OIG as appropriate will coordinate reporting to the Federal Protective Service, the local police, or other law enforcement authority with jurisdiction. Similar incidents occurring outside of Federal facilities must first be reported to the local police that has jurisdiction and to the OIG upon returning to the office. Government approved Smart Phone devices lost or stolen outside of GSA Federal facilities are not required to be reported to local police but must be reported to the OIG upon returning to the office. To report an incident, call the national hotline at 1(800) 424-5210 (Toll free). In addition, the incident should always be reported to the IT Service Desk. All incidents involving personally identifiable information in electronic or physical form must be reported to the GSA OCISO via the IT Service Desk within one hour of discovering the incident. GSA employees, contractors, and authorized users shall report all incidents to the IT Service Desk. There should be no distinction between suspected and confirmed

breaches. The OCISO shall promptly notify the GSA OIG of any incidents involving personally identifiable information.

(5) Data breaches (i.e., loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users with an authorized purpose have access or potential access to Personally Identifiable Information, whether physical or electronic) shall follow reporting and response procedures as defined in GSA Order CIO 9297.2B, GSA Information Breach Notification Policy. Refer to GSA Order CIO 9297.1 GSA Data Release Policy, for non-releasable information to the public or persons other than the employee, except when required by law (e.g., court order). See also Chapters 7 and 8 of GSA Order CIO P 2180.1, GSA Rules of Behavior for Handling Personally Identifiable Information (PII).

(6) FIPS 199 Moderate and High impact systems must annually test the security incident response capability to determine the incident response effectiveness.

j. Security advisory alert handling.

(1) Office of the CISO must create procedures to share common threats, vulnerabilities, and incident related information with the appropriate organizations.

(2) ISSMs and ISSOs must report on the status of security advisory alerts to the Office of the CISO upon request.

k. Media protection.

(1) All GSA data from information system media, both digital and non-digital must be sanitized in accordance with methods described in IT Security Procedural Guide: Media Protection Guide, OCIO-IT Security-06-32, before disposal or transfer outside of GSA.

(2) Restrict access to information system media (e.g., disk drives, diskettes, internal and external hard drives, and portable devices), including backup media, removable media, and media containing sensitive information to authorized individuals.

(3) Physically control and securely store information system media within controlled areas.

(4) Protect digital media during transport outside of controlled areas using a certified FIPS 140-2 encryption module; non-digital media shall follow GSA personnel security procedures.

l. Configuration management.

(1) A system configuration management plan must be developed, implemented, and maintained for every IT system managed by GSA.

(2) All information systems must be securely hardened and patched before being put into operation and while in operation.

(3) GSA information systems, including vendor owned / operated systems on behalf of GSA, must configure their systems in agreement with GSA technical guidelines, NIST guidelines, Center for Internet Security guidelines (Level 1), or industry best practice guidelines, as deemed appropriate. Where a GSA benchmark exists, it must be used. GSA benchmarks may be exceeded but not lowered.

(4) Develop the configuration management plan IAW GSA-CIO-IT-Security-01-05.

m. Firewall access.

(1) The Office of the Chief Information Security Officer must approve all requests for access through the GSA Firewall. Firewall change requests must follow the process outlined in IT Security Procedural Guide: Firewall Change Request, OCIO-IT Security-06-31. This includes changes to desktop firewall and intrusion prevention systems.

(2) The Office of the Chief Information Security Officer will block access to all external sites deemed to be a security risk to GSA. Exceptions to this policy must be approved by the CISO.

Note: Detailed guidance regarding firewall access is available in GSA-CIO-IT-Security-06-31: Firewall Change Request.

n. Monitoring.

(1) Obtaining access to GSA resources must constitute acknowledgment that monitoring activities may be conducted.

(2) Users have no expectation of privacy on GSA IT systems. All activity on GSA IT systems is subject to monitoring.

(3) All GSA IT systems must display an approved warning banner to all users attempting to access GSA's computer systems indicating the system is subject to monitoring.

(4) Controls shall be put in place to monitor or detect changes or updates to systems that are outside the parameters of a system's baseline operating characteristics. This includes the ability to monitor resource usage and allocation.

(5) Audit user activity for indications of fraud, misconduct, or other irregularities.

(6) Document all phases of monitoring activity including:

(a) Monitoring procedures. The procedures must include specific steps to be taken and protocol to be applied when reviewing audit data.

(b) Response procedures. Procedures must be documented for responses to detected irregularities.

(c) Review of user activity. Thorough documentation on reviews conducted on audit data must be generated and stored IAW the GSA Record Management Program or for not less than 3 years.

Note: Detailed guidance regarding monitoring is available in GSA-CIO-IT-Security-12-63: System and Information Integrity, GSA-CIO-IT-Security-01-02: Incident Response, GSA-CIO-IT-Security-01-05: Configuration Management, GSA-CIO-IT-Security-01-08: Audit and Accountability, GSA-CIO-IT-Security-01-07: Access Control.

o. Software and digital media acceptable use.

(1) Users of GSA IT resources must use only software that is properly licensed and registered for GSA use.

(2) All GSA users must abide by software and digital media copyright laws and must not obtain, install, replicate, or use unlicensed software and digital media.

(3) Users of GSA IT resources must obtain all software from GSA sources and must not download software from the Internet without prior permission from the appropriate ISSO, as downloading software from the Internet may introduce viruses/worms to the GSA network.

(4) Users must not install any software or hardware without approval through the EARC process.

(5) Users must not acquire, possess, trade, or use hardware or software tools that could be employed to evaluate or compromise GSA resources unless authorized by the appropriate ISSO. Examples of such tools include those that defeat software copy protection, discover passwords, identify security vulnerabilities, or decrypt encrypted files.

(6) Users must not install, download, or run peer-to-peer software. Software that has peer-to-peer file sharing technology built in may be approved by OCISO if the file sharing functionality has been limited or disabled.

p. E-mail, social media and internet acceptable use.

(1) GSA provides access to e-mail and Social Media for Government business. However, users may occasionally make personal use of e-mail and Social Media that involves minimal expense to the Government and does not interfere with government business. Prior to establishing an official GSA Social Media presence, users must inform the Office of Communications and Marketing's (OCM) Enterprise Web Management (EWM) group which can monitor and assist with GSA branding and other aspects related to dealing with the public.

(2) Users must not use e-mail or Social Media for any activity or purpose involving classified data.

(3) Users must avoid the following prohibited e-mail and Social Media usages:

(a) Transmitting unsolicited commercial announcements or advertising material, unless approved by management in advance.

(b) Transmitting any material pertaining to GSA, the Federal Government, or any agency employee or official that is libelous or defamatory.

(c) Transmitting sexually explicit or offensive material, non-business related large attachments, chain letters, un-authorized mass mailings, or intentionally sending a virus/worm.

(4) Personal use of Government IT systems for Internet access must be kept to a minimum and must not interfere with official system use or access.

(5) Users must avoid prohibited Internet usages including:

(a) Unauthorized attempts to break into any computer, whether belonging to GSA or another organization.

(b) Browsing sexually explicit, gambling sites or hate-based web sites.

(c) Using Internet access for personal gain (i.e., making use of GSA resources for commercial purposes or in support of for profit activities such as running a private business).

(d) Theft of copyrighted or otherwise legally protected material, including copying without permission.

(e) Sending or posting sensitive material such as GSA building plans or financial information outside of the GSA network.

(f) Automatically forwarding e-mail messages from GSA e-mail addresses to any non-Federal e-mail account(s) or address(es).

(g) Sending e-mail messages including sensitive information, such as PII, as deemed by the Data Owner, without GSA provided encryption. Certified encryption modules must be used IAW FIPS PUB 140-2, Security requirements for Cryptographic Modules.

(6) If PII needs to be e-mailed outside the GSA network encryption is required. Instructions can be found on the privacy web page in the section "Documents for Download." Your e-mail will be blocked if Social Security Numbers are sent unencrypted.

(7) GSA prohibits an employee or contractor supporting GSA from creating or sending information using a non-official GSA electronic messaging account unless: (1) copies of the message is sent to an official GSA electronic messaging account of the employee or contractor in the original creation or transmission of the record, or (2) a complete copy of the message or record is forwarded to an official GSA electronic messaging account of the employee or contractor not later than 20 days after the original creation or transmission of the record. Additional guidance regarding GSA E-Mail Policy is available in GSA Order CIO 2160.2 GSA Electronic Messaging and Related Services. GSA Order ADM 7800.11, Personal Use of Agency Office Equipment. GSA Order CIO 2104.1, GSA Information Technology (IT) General Rules of Behavior and GSA Order CIO P 2165.1, GSA Internal Telecommunications Management. Detailed guidance on Social Media is available in The Social Media Navigator, GSA's Guide to the Use of Social Media, April 2011 or current.

q. Portable storage devices.

(1) All agency data on portable storage devices (e.g., USB flash drives, SD cards, external hard drives) must be encrypted with a FIPS 140-2 certified encryption module.

(2) Users shall follow the requirements of Chapter 4, Paragraph i, Subparagraph 4 of this chapter with regard to PII or other data deemed sensitive by the Data Owner.

(3) Users must secure portable storage devices using the same policies and procedures as paper documents as proscribed by the Office of Human Resources Management (OHRM) policies.

(4) Users must protect portable storage devices in the same manner as a valuable personal item and should not leave unattended in public places, automobiles, etc.

(5) Users must immediately report lost or stolen portable storage devices to the appropriate ISSO or IT Service Desk. Reference Chapter 4, Paragraph i, Subparagraph 5 for reporting requirements to the OIG.

r. Mobile devices (smartphones/tablets). GSA users must secure mobile devices, like all enterprise devices, against a variety of threats. This includes handling PII as described in Chapter 4, Paragraph 4, subparagraph w of this chapter, securing the devices, and reporting lost or stolen devices. Included in the definition of 'Mobile devices' are smartphones and tablets. Excluded in the definition of mobile devices are laptops since the security controls for laptops are quite different from smartphones. Also excluded in the definition are basic cell phones due to the limited security options available and their limited threat. GSA has outlined information on mobile devices at: https://sites.google.com/a/gsa.gov/mobileinfo/. The *IT Security Procedural Guide: Securing Mobile Devices and Applications, CIO-IT Security-12-67* is designated as the GSA Policy on mobile devices and applications and provides specific information, including:

(1) Government issued devices.

(a) GSA uses centralized mobile device management (MDM) to manage the configuration and security of mobile devices. GSA provisions and activates MDM on each mobile device before issuing to users.

(b) GSA organizations must define procedures to periodically monitor mobile device security to verify compliance with GSA requirements.

(c) GSA's MDM ensures appropriate security including: encryption, application controls, passwords usage, remote locking, remote wiping, operating system protection.

(d) Users must not connect to GSA resources without complying with the requirements which the Guide describes.

(2) Personally owned mobile devices.

(a) GSA has implemented a Bring Your Own Device (BYOD) policy that allows users to connect non-GSA procured devices to GSA resources.

(b) IT Security Procedural Guide: Securing Mobile Devices and Applications, CIO-IT Security-12-67 is designated as the GSA policy on mobile devices and applications, and details the steps necessary to use a personally owned mobile device, which include:

1. GSA will install MDM on the device and enforce control security settings, including password usage, encryption, and inactivity timeout.

2. GSA will ensure that GSA can wipe the device clean if it is lost or stolen or after repeated unsuccessful attempts at logon.

3. GSA will not support personally owned mobile devices.

4. Users must agree to and sign a GSA Personal Device Usage Agreement and the GSA Rules of Behavior for Personally Owned Mobile Devices.

s. Peer-to-peer networking and instant messaging.

(1) The installation or use of peer-to-peer networking software is prohibited on GSA computers and the GSA network. Software that has peer-to-peer file sharing technology built in may be approved by OCISO if the file sharing functionality has been limited or disabled.

(2) The installation or use of unauthorized instant messaging (IM) software is prohibited. (i.e., must use an approved GSA standard).

t. Separation of duties (FIPS 199 Moderate and High Impact Systems Only).

(1) Responsibilities with a security impact must be shared among multiple staff by enforcing the concept of separation of duties, which requires that individuals do not have control of the entirety of a critical process.

(2) Define and implement detailed separation of duties policies for IT systems based on the specific processes, roles, permissions, and responsibilities of personnel involved in departmental business operations.

(3) Every S/SO/R must consider how a separation of duties conflict can arise from shared access to applications and systems. Specifically, application programmers and configuration management personnel should not generally have concurrent access to the development and production environment. Failure to segregate access to source code and production code increase the risk that unauthorized modifications to programs may be implemented into production systems, which could introduce vulnerabilities and negatively impact the integrity and availability of data generated and stored in the system.

(4) Document job descriptions and roles to accurately reflect the assigned duties, responsibilities, and separation of duties principles. By clearly documenting position responsibilities and functions, employees are positioned to better execute their duties IAW policy.

(5) Establish formal procedures to guide personnel in performing their duties, with identification of prohibited actions.

(6) Duties shall be segregated among users so that the following functions shall not generally be performed by a single individual:

(a) Data entry and verification of data. Any data entry or input process that requires a staff member to inspect, review, audit, or test the input to determine that the input meets certain requirements should not permit the same individual to both enter and verify the data. The objective is to eliminate self-certification or verification of data input or entry procedures. Note that this could be an automated or manual process and is not limited to financial transactions.

(b) Data entry and its reconciliation to output. Any data entry or input process that requires reconciliation or matching of transactions to identify discrepancies should not permit the same individual to both enter and reconcile data.

(c) Input of transactions for incompatible processing functions (e.g., input of vendor invoices and purchasing and receiving information).

(d) Data entry and supervisory authorization functions (e.g., authorizing a rejected transaction to continue processing that exceeds some limit requiring a supervisor's review and approval).

(7) Ensure proper separation of duties for GSA IT system maintenance, management, and development processes.

(8) Information systems must enforce separation of duties through assigned access authorizations.

(9) Since critical processes can span separate and distinct applications and systems, each Service, Staff Office, and Region (S/SO/R) will take a macro view of existing roles to define and establish incompatibilities and separation of duties conflicts across an entire business process. This means examining roles that may span multiple IT systems or applications to uncover conflicts that may not be immediately apparent (e.g., an individual has permissions to create and/or modify vendor data in a General Ledger system and the ability to create invoices and purchase orders in an Accounts Payable system).

(10) Every S/SO/R must establish physical and logical access controls to enforce separation of duties policy and alignment with organizational and individual job responsibilities.

(11) Conduct annual assessments to review the effectiveness of control techniques, with an emphasis on activities that cannot be controlled through logical, physical, or compensating controls. The reviews determine whether in-place control techniques are maintaining risks within acceptable levels (e.g., periodic risk assessments).

(12) Review access authorization listings to determine whether they remain appropriate at least annually.

(13) Conduct annual reviews of staff training records to ensure annual Privacy Act, Security Training, and application specific training was completed for all users. The records shall be forwarded to application ISSO/System Owners as part of the annual recertification efforts.

u. Least privilege.

(1) Information systems must operate in such a way that they run with the least amount of system privilege needed to perform a specific function and that system access is granted on a need to know basis.

(2) Privileged rights including but not limited to “administrator,” “root,” and “power user’ shall be restricted to authorized employees and contractors as approved by the AO.

(3) Information systems must be configured to the most restrictive mode consistent with operational requirements and IAW appropriate procedural guides from NIST and/or GSA to the greatest extent possible. Implemented configuration settings should be documented and enforced in all subsystems of the information system.

v. Remote access/end point security.

(1) All desktop or laptop computers, including personal devices, connecting remotely to GSA must have anti-virus software running with the latest signature files, a firewall installed and running, and all security patches installed. Failure to have current security signatures or patches may result in loss of access to the GSA network or data.

(2) All computers accessing GSA through a GSA Secure Sockets Layer (SSL) or Internet Protocol Security (IPsec) Virtual Private Network (VPN) must allow an endpoint device that checks for the presence of a client firewall, up to date virus protection software and up to date patches. The endpoint device must also verify the absence of malicious software (e.g., Trojans, worms, malware, spyware, etc.) on the client machine. Machines that fail this scan will not be allowed access to the GSA network or any GSA IT resources.

(3) Only GSA GFE that is determined to be properly secured (based on the scans noted above) will be allowed unrestricted remote access to the GSA network.

(4) Personal computers and/or contractor computers will only be allowed access to the Citrix Netscaler and will not have the ability to map local drives (contingent on passing the security scans noted in paragraph b). No PII or other data deemed sensitive by the Data Owner shall be stored on non-GFE.

(5) In special cases for remote administration and maintenance tasks, contractors will be allowed restricted IPSEC access to specific GSA IP addresses (contingent on passing the security scans noted in paragraph b).

w. Personally Identifiable Information (PII). The following security requirements apply to the protection of PII.

(1) If it is a business requirement to store PII on GSA user workstations or mobile devices including, but not limited to notebook computers, USB drives, CD-ROMs/DVDs, personal digital assistants, PII must be encrypted using a FIPS 140-2 certified encryption module. An employee or contractor shall not physically take PII from GSA facilities (including GSA managed programs housed at contractor facilities under contract), or access remotely (i.e., from locations other than GSA facilities), without written permission from the employee's supervisor, the Data Owner, and the IT system Authorizing Official. Approvals shall be filed with the employee's supervisor. This applies to electronic media (e.g., laptops, USB drives), paper, and any other media (e.g., CDs/DVDs) that may contain PII.

(2) PII shall be stored on network drives and/or in application databases with proper access controls (i.e., User ID/password) and shall be made available only to those individuals with a valid need to know.

(3) Log all computer-readable data extracts from databases holding PII and verify each extract including PII that has been erased within 90 days or if its use is still required.

(4) Creation of computer-readable data extracts that include PII shall be maintained in an official log including creator, date, type of information, and user.

(5) If PII needs to be transmitted over the Internet, it must be sent using encryption methods defined in Chapter 5, Paragraph 2, Subparagraph g of this IT security policy.

(6) Data breaches (i.e., loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users with an authorized purpose have access or potential access to Personally Identifiable Information, whether physical or electronic) shall follow reporting and response procedures as defined in GSA Order CIO 9297.2B, GSA Information Breach Notification Policy. Refer to GSA Order CIO 9297.1 GSA Data Release Policy, for non-releasable information to the public or persons other than the employee, except when required by law (e.g., court order). See also Chapters 7 and 8 of GSA Order CIO P 2180.1, GSA Rules of Behavior for Handling Personally Identifiable Information (PII).

(7) GSA managed computers that collect and store PII must adhere to all PII requirements.

(8) If PII needs to be e-mailed outside the GSA network encryption is required. Instructions can be found on the privacy web page in the section "Documents for Download." Your e-mail will be blocked if Social Security Numbers are sent unencrypted.

(9) If PII needs to be sent by courier, printed, or faxed several steps should be taken. When sending PII by courier mark "signature required" when sending documents. This creates a paper trail in the event items are misplaced or lost. Don't let PII documents sit on a printer where unauthorized employees or contractors can have access to the information. When faxing information, use a secure fax line. If one is not available, contact the office prior to faxing, so they know information is coming, and contact them after transmission to ensure they received it. For each event the best course of action is limit access of PII only to those individuals authorized to handle it, create a paper trail, and verify information reached its destination.

(10) Comply with security and privacy awareness training requirements for employees and contractors (internal and external). All employees and contractors shall complete “IT Security Awareness and Privacy 101 Training,” “Privacy Training 201,” and the “Sharing in a Collaborative Environment” training before being provided access to any PII, as defined in OMB Memorandum M-07-16 and M-10-23.

(11) Ensure employees and contractors have the proper background investigation before accessing PII.

(12) Employees and contractors may access PII remotely [i.e., remote access is when the individual is not physically located in a GSA facility (e.g., when the individual is teleworking)] unless explicitly prohibited by the GSA Senior Agency Official for Privacy (SAOP) and/or the Authorizing Official (AO) for the particular information system, in coordination with the Data Owner and/or the GSA Supervisor. All access shall only be from Government Furnished Equipment (GFE) or through an approved GSA virtual interface (i.e. Citrix and/or VDI). In addition, an individual shall not download or store PII on non-GFE. Approval to telework is at the discretion of the GSA -Supervisor and/or Contracting Officer, as applicable, and in conformance with GSA Order HCO 6040.1A.

(13) Employees and contractors shall have a favorable initial fitness/suitability determination and be in the process of receiving a Minimum Background Investigation (or comparable investigation) or higher to access PII. The authority and access shall be determined by the appropriate GSA Supervisor (for GSA employees) or Contracting Officer (for contract personnel), Data Owner, and the System's Authorizing Official (AO). Each System's AO, with the request of the GSA Supervisor, Data Owner or Contracting Officer, shall evaluate the risks associated with each such request. To find Authorizing Officials go to https://ea.gsa.gov/ and click on “Security” then “FISMA Systems – POC.”

(14) There shall be no waivers to background investigations for IT access for GSA employees or contractors. A favorable initial fitness/suitability determination shall be granted before access to the GSA network or any GSA IT system.

(15) Employees and contractors working with PII shall verify callers' identity before discussing or providing any PII to individuals on the telephone. The verification technique shall be documented and approved by the GSA SAOP in advance of the discussion or provision of any PII.

(16) Data breaches (i.e., loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users with an authorized purpose have access or potential access to Personally Identifiable Information, whether physical or electronic), shall follow reporting and response procedures as defined in GSA Order CIO 9297.2B. GSA Information Breach Notification Policy. Refer to GSA Order CIO 9297.1 GSA Data Release Policy for non-releasable information to the public or persons other than the employee, except when required by law (e.g., court order). See also Chapters 7 and 8 of GSA Order CIO P 2180.1. GSA Rules of Behavior for Handling Personally Identifiable Information (PII).

x. Guest wireless access.

(1) A GSA Guest Wireless Network has been established in the Regional and Central Office Buildings to allow non-Government Furnished Equipment (GFE) access only to the Internet and GSA resources that are available to the general public (www.gsa.gov). It is intended to be a service for customers of the agency, as well as vendors performing official business on site.

(a) Guest wireless accounts are not ENT accounts.

(b) The User ID will change weekly

(c) The Password is posted on InSite.

(d) The password will be changed monthly.

(e) Guest wireless traffic will be subject to the same content filtering as traffic on the production network.

(2) All non-GFE/workstations connected to the GSA Network shall only be allowed access to the Internet (example: .guest network only, no access allowed to the GSA resources).

y. International travel policy for Portable Electronic Devices (PED). The widespread use of PEDs as stand-alone, networks and remote access devices, present special security concerns not limited to laptops, cell phones, thumb drives, Personal Data Assistants (PDA), tablets, and pagers. Vulnerabilities of these devices while on international travel warrant specific controls to protect the GSA network. GFE must not be taken on international travel without prior approval from the individual's supervisor and OMA.

(1) Individuals with a Top Secret/Sensitive Compartmented Information (TS/SCI) clearance must contact OMA prior to any international travel.

(2) OMA will provide direction on foreign contact, security precautions, mobile devices, etc.

(3) GSA employees (with the exception of the OIG employees) that hold a National Security clearance, and at the discretion of OMA, shall be issued loaner devices by GSA IT when traveling outside the United States or European Union, or any area deemed to have an elevated risk during the period of travel. The loaner devices must be returned to GSA IT immediately upon the employee's return. These loaner devices shall be wiped immediately by GSA IT to ensure no data remains resident on the system(s) issued. Due to technical security controls in place for all mobile devices (encryption and, mobile device management), personnel in Public Trust positions are not required to follow this provision unless deemed to be required by OMA to provide additional safeguards to data these personnel may access.

CHAPTER 5: POLICY ON TECHNICAL CONTROLS

This chapter provides the basic technical control security policy statements for GSA systems. Technical Controls provide specific guidance on security controls and technical procedures used to protect GSA IT resources. The policy statements are derived primarily from OMB Circular A-130 and are integral to an effective IT security program. The manner in which these controls are implemented depends on the risks, sensitivity, and are criticality associated with the specific systems and data involved. In some cases, basic security policy controls may need to be modified or supplemented in order to address application-specific or system-specific requirements.

1. According to NIST, the Technical Controls are obtained from the following Control Families:

- Access Control (AC)
- Audit and Accountability (AU)
- Identification and Authentication (IA)
- System and Communications Protection (SC)

2. The following paragraphs provide specific policy on controls for identification and authentication, access control, auditing, and others.

a. Identification and authentication. All GSA systems must incorporate proper user identification and authentication methodology. Refer to the GSA-CIO-IT-Security-01-01: Identification and Authentication Procedural Guide for additional details. For mobile devices, refer to Chapter 4.

(1) Authentication schemes for Moderate and High Impact systems must utilize multifactor authentication using two or more types of identity credentials (e.g. passwords, SAML 2.0 biometrics, tokens, smart cards, one time passwords) as approved by the Authorizing Official and in accordance with the security requirements in the subparagraphs of this paragraph.

(2) An authentication scheme using passwords as a credential must implement the following security requirements:

(a) Passwords must contain a minimum of eight (8) characters which include a combination of letters, numbers, and special characters. Accounts used to access USGCB compliant workstations must contain a minimum of sixteen (16) characters but do not have to contain a combination of letters, numbers, and special characters.

(b) Information systems must be designed to require passwords to be changed every 90 days.

(c) Information systems must automatically lockout users after not more than ten (10) failed access attempts during a 30 minute time period. Accounts must remain locked for a minimum of 30 minutes for the next login prompt.

(d) Passwords for all mobile devices such as GSA approved smart phones, iPads, and tablets must be a minimum of 6 characters. The six character password requirement also applies to personal mobile devices accessing GSA data or systems.

(e) Passwords must not be stored in forms (i.e. Windows dialog boxes, web forms, etc.).

(f) All default passwords on network devices, databases, operating systems, etc. must be changed.

(g) Other than default or one time use passwords, passwords must never be sent via e-mail, regular mail, or interoffice mail.

(h) User IDs and passwords must never be distributed together (i.e. same e-mail, regular mail, interoffice mail, etc.).

(i) Users must be authenticated before resetting or distributing a password.

(4) Systems with an authentication assurance level of 2 or above, used by federal employees or contractors must accept federal Personal Identity Verification (PIV) cards and verify them in accordance with guidance in OMB M-11-33.

(5) All users issued Government Furnished Equipment are required to log into the workstation using a GSA issued PIV credential. The following groups of users are exempt from this requirement:

(a) A Federal employee on detail to GSA, issued a PIV from the employees assigned Agency

(b) Any employee or contractor expected to be employed for less than 180 days and not issued a PIV

(c) Any person with a disability that does not allow the individual to utilize a PIV card and laptop.

(d) Any user with a PIV that is lost, forgotten at home, or damaged in any way, may contact the IT Service Desk (ITSD) to request a temporary exception to the above requirement, not to exceed forty-five (45) days.

(6) Systems with users who are agency business partners or the general public, and who register or log into the system, must accept credentials issued by identity providers who have been certified by federally approved Trust Framework Providers.

(7) Authentication methods for applications and systems may use the authentication mechanisms provided by the general support system if deemed appropriate by the Authorizing Official.

(8) E-commerce and publicly accessible systems must incorporate identification and authentication mechanisms commensurate with their security risks and business needs and may differ from the security requirements set forth by this policy. In such cases the identification and authentication mechanisms must be approved by the AO in writing and concurred by the OCISO.

(9) One time use passwords must expire in twenty-four (24) hours.

(10) User IDs and passwords must never be distributed together, whether in the same e-mail, via interoffice mail, or postal mail.

(11) Users must be authenticated before resetting or distributing a password.

(12) User IDs shall be unique to each authorized user.

(13) All GSA workstation and mobile devices shall initiate a session lock after 15 minutes of inactivity. The session lock shall remain in effect until the user reestablishes access using appropriate identification and authentication.

(14) FIPS 199 Moderate and High impact systems shall automatically terminate temporary and emergency accounts after no more than ninety (90) days.

(15) FIPS 199 Moderate and High impact systems shall automatically disable inactive accounts after ninety (90) days.

(16) FIPS 199 Moderate and High impact systems shall automatically terminate a remote access connection and Internet accessible application session after thirty (30) minutes of inactivity. The time will be thirty (30) – sixty (60) minutes for non-interactive users. Static web sites, long running batch jobs and other operations are not subject to this time limit.

(17) Web sites (internal and public) with logon functions, must implement TLS encryption with a FIPS 140-2 validated encryption module. SSL/TLS implementation must be IAW SSL / TLS Implementation Guide [CIO-IT Security-14-69]

(18) GSA has implemented a “Bring Your Own Device (BYOD)” policy in (CIO-IT-Security-12-67) that allows users to connect their non-GSA procured smartphones and tablets, which have been previously approved by IT security, to GSA resources in a native fashion. The following IA-related guidelines outline the current BYOD Policy for GSA employees and contractors:

(a) The mobile device shall automatically lockout within 15 minutes of inactivity. The session lock shall remain in effect until the user reestablishes access using appropriate identification and authentication.

(b) The device will automatically wipe after 10 unsuccessful attempts at logon.

(c) The device will maintain a minimum passcode length of 6 characters.

b. Logical access controls.

(1) All GSA systems must implement logical access controls to authorize or restrict the activities of users and system personnel to authorized transactions and functions.

(2) Public users must be restricted to using designated public services.

(3) Information system accounts must be managed for all systems, including establishing, activating, modifying, reviewing, disabling, and removing accounts. Reviews and validations of system users' and staff users' accounts shall be completed annually to ensure the continued need for system access.

(4) Information systems must enforce the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.

Note: Detailed guidance regarding access controls is available in GSA-CIO-IT-Security-01-07: Access Control.

c. Audit records.

(1) Security-activity auditing capabilities must be employed on all GSA information systems using IT Security Procedural Guide: Auditing & Monitoring, OCIO-IT Security-01-08 and NIST SP 800-37 as guides.

(2) Audit records must be regularly reviewed/analyzed for indications of inappropriate or unusual activity. Suspicious activity or suspected violations must be investigated. Any findings must be reported to appropriate officials IAW IT Security Procedural Guide: Incident Response, OCIO-IT Security-01-02.

(3) Intrusion detection systems must be implemented as deemed appropriate by the Authorizing Official.

(4) Information systems must alert appropriate organizational officials in the event of an audit processing failure and take one of the following additional actions:

shut down information system, overwrite oldest audit records, or stop generating audit records.

(5) Information systems must produce audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.

(6) Audit log data must be archived for a period of not less than 180 days.

(7) Systems that contain permanent electronic records must be maintained in an electronic format by 12/31/2019.

(8) All permanent and temporary e-mail records must be accessible electronically in an electronic format.

Note: Detailed guidance regarding auditing is available in GSA-CIO-IT-Security-01-08: Audit and Accountability.

d. Warning banners/system use notification message.

(1) All internal GSA IT systems must display an approved warning banner to all users attempting to access GSA's computer systems. The warning banner must read as follows:

**********WARNING**********
This is a U.S. General Services Administration Federal Government computer system that is "FOR OFFICIAL USE ONLY." This system is subject to monitoring. Therefore, no expectation of privacy is to be assumed. Individuals found performing unauthorized activities are subject to disciplinary action including criminal prosecution.

(2) For publicly accessible sites (i.e., open to the Internet) the sentence, "Therefore, no expectation of privacy is to be assumed" shall be removed. Detailed guidance regarding access controls is available in GSA-CIO-IT-Security-01-07: Access Control.

e. Remote access. Access to the GSA domain must be restricted to secure methods using approved identification and authentication methods that provide detection of intrusion attempts and protection against unauthorized access.

(1) Individuals other than GSA employees and contractor personnel are not allowed to use GSA furnished computers, GSA VPN connection, or a GSA provided or funded internet connection.

(2) Users must not connect to other computers or networks via modem while simultaneously connected to the GSA network (i.e., no dialing outbound to your Internet Service Provider or allowing inbound calls to your computer while at the same time

being connected to GSA's network). However, accessing GSA's network via the GSA-provided VPN software is allowed.

(3) When using the GSA IT IPsec VPN, users must connect using only IP and must have the client firewall bound to all network adapters.

(4) Allow remote access only with multifactor authentication where one of the factors is provided by a device separate from the computer gaining access. All remote access connections shall automatically terminate within 30 minutes of inactivity.

Note: Detailed guidance regarding access controls is available in GSA-CIO-IT-Security-01-07: Access Control.

f. Vulnerability testing.

(1) GSA CIO, Service/Staff Offices, or Regions shall conduct vulnerability scanning of operating systems, information systems, databases, and web applications at least quarterly or when significant new vulnerabilities potentially affecting the system are identified and reported. All critical and high vulnerabilities identified must be mitigated within 30 days and all moderate vulnerabilities mitigated within 90 days IAW IT Security Procedural Guide: Managing Enterprise Risk, OCIO-IT-06-30.

(2) Independent vulnerability testing including penetration testing and system or port scanning conducted by a third party such as the GAO and other external organizations must be specifically authorized by the Authorizing Official and supervised by the ISSM.

(3) GSA S/SO/Rs shall scan for unauthorized wireless access points quarterly and take appropriate action if such an access point is discovered.

g. Encryption.

(1) All passwords must be encrypted in storage.

(2) All sensitive information, such as PII, as deemed by the Data Owner, which is transmitted outside the GSA firewall, must be encrypted. Certified encryption modules must be used IAW FIPS PUB 140-2, Security requirements for Cryptographic Modules. Your e-mail will be blocked if Social Security Numbers are sent unencrypted.

(3) When using password generated encryption keys, a password of at least 8 characters with a combination of letters, numbers, and special characters is required. A password of at least 12 characters is recommended.

(4) Systems implementing encryption must follow the key management procedures and processes documented in IT Security Procedural Guide: Key Management, OCIO-IT Security-09-43.

h. New technologies. All new technology developments, designs, and implementations shall use industry best practices, Government guidelines, and Government audit findings as they become available. Examples of new technologies include Internet Protocol v6 (IPv6) and Voice over IP (VoIP). VoIP must use NIST SP 800-58 Security considerations for Voice over IP Systems as a guide.

i. Malicious code protection. All information systems must implement and enforce a malicious code protection program designed to minimize the risk of introducing malicious code (e.g., viruses, worms, spyware, Trojan horses) into agency systems and networks.

j. Patch management. System administration and patch implementation must be restricted to authorized personnel.

k. Website privacy policy statement. Every Federal web site (internal and public) must include a privacy policy statement, even if the site does not collect any information that results in creating a Privacy Act record. Reference OMB Memorandum M-99-18, Privacy Policies on Federal Web Sites, for guidance and model language on privacy statements.

l. Account management.

(1) Request and approval routing in support of account management processes must assure:

(a) All access requests require at least one supervisor approval. Access requests submitted directly from a user must not be accepted, regardless of position;

(b) Users complete and send access requests to their supervisor or Contracting Officer Representative (COR), not directly to the Data or System Owner;

(c) Access requests may be aggregated and managed by designated coordinators for efficiency;

(d) Access requests are routed to the data or System Owner by a user's supervisor, COR, ISSO, ISSM, director, or designated regional coordinator.

(2) Authorizations supporting the account management processes must assure:

(a) Supervisors are responsible for coordinating and arranging system access requests for all new or transferring employees and for verifying an individual's need-to-know.

(b) Data Owners/System Owners, with assistance from the designated ISSO, ensure system access is restricted to authorized users that have completed required background investigations, are familiar with internal security practices, and

have completed requisite security and privacy awareness training programs, such as the annual Information Security & Privacy Act training curriculum. System access authorizations must enforce job function alignment, separation of duties, and be based on the principle of need-to-know. Contractors with system access must utilize a gsa.gov e-mail account to conduct business with GSA.

(3) Establishment and activations supporting the account management processes must assure:

(a) Data or System Owner grants access to the information system based on a valid need-to-know/need-to-share that is determined during the account authorization process and the intended system usage.

(b) The delegation of user roles or permissions for applications, in particular those containing Personally Identifiable Information (PII) and/or sensitive financial data, must be compliant with the principles of least privilege, separation of duties, and need-to-know.

(c) Accounts are created only upon receipt of valid access requests conforming to the GSA access request protocol.

(4) Update and modification of user accounts supporting account management processes must ensure:

(a) Supervisors are responsible for coordinating and arranging system access modifications for personnel.

(b) Users complete and send account update requests directly to his or her supervisor or COR, not directly to the Data or System Owner.

(c) Update requests are aggregated and managed by designated regional coordinators for efficiency.

(d) Update requests are routed to the Data or System Owner by a user's supervisor, COR, director, or designated regional coordinator.

(5) Disabling and removal of user accounts supporting account management processes must ensure:

(a) Supervisors are responsible for coordinating and arranging system access termination for all departing or resigning personnel.

(b) Account removal is initiated by a user's supervisor, COR, or through the review of the monthly OHRM separation list submitted by the OCISO.

(c) Removal requests may be aggregated and managed by designated regional coordinators for efficiency.

(d) Termination and transfer procedures must be incorporated into the authorization process for all information systems.

(6) User authorizations must be verified annually for all information systems.

(7) User account privileges must be reviewed across the appropriate Service, Staff Office, and Region application portfolio to assess incompatible and non-compliant role assignments (e.g., review of user access assignments across multiple significant systems that share data or pass transactions to identify conflicts with separation of duties policy).

(8) On a regular basis, Data and System Owners must inspect user access entitlements as needed to detect the following conditions that warrant termination, revocation, or suspension of account access:

(a) Orphaned accounts. An orphaned account is defined as a user account that has demonstrated, or is expected to demonstrate, an extensive period of idle time consistent with account abandonment.

1. FIPS 199 Moderate and High impact systems shall automatically disable inactive accounts after 90 days and shall automatically terminate temporary and emergency accounts after no more than 90 days;

2. Upon issuance of the CISO monthly separation reports, Data and System Owners must verify within 30 days that separated personnel no longer maintain access to GSA IT systems or resources.

(b) Role conflicts. Any accesses or permissions that clearly violate established separation of duties policies must be coordinated with the designated S/SO/R ISSO to correct or resolve conflicting role assignments.

(c) Shared accounts. Shared user accounts violate the principles of separation of duties and non-repudiation, and must be detected and suspended when discovered.

(d) Suspension or revocation of GSA e-mail accounts. Systems that require users to maintain an active e-mail account must suspend or revoke access for users whose e-mail credentials are no longer valid.

m. Trusted Internet Connection (TIC). All network devices that are either owned, managed, maintain a connection to a GSA facility, and/or handle GSA data shall be strategically positioned behind a GSA firewall to provide analysis/correlation, management structure, and minimize threats presented by external attacks. TIC will

allow GSA to provide the following security functions for any devices connected to GSA networks:

(1) Monitoring, incident response, vulnerability assessment, vulnerability management, incident reporting, engineering support, and the enforcement of the agency's specific security policy at the hosted facility.

(2) Trained, qualified, and cleared staff to; support security functions 24x7.

(3) Limited inbound and outbound connections so that only necessary services are allowed.

(4) Centralized, secured, and unified management of security events in order to protect the integrity of Government data and its infrastructure.

n. Bluetooth keyboards, mice and headsets.

(1) Bluetooth is approved for use with keyboards, mice and headsets on GSA GFE. The following restrictions apply:

(a) Devices must use the Bluetooth Protocol version 1.2 or later. If the device was manufactured 2005 or later, the version must be confirmed by consulting the device specifications.

(b) If a password/PIN must be chosen for device pairing the user should use a combination of letters and numbers when possible. A four digit pin should not be used unless this has been hardcoded by the manufacturer. Users should also use a different pass code/PIN for each pairing.

(2) The computer/device should not be discoverable except as needed for pairing. Discoverable mode (also known as "visible mode" or "pairing mode") is the mode that allows the pairing of two Bluetooth devices. Uses must ensure discoverable mode is disabled after pairing is completed.

(3) Bluetooth capabilities must be disabled when they are not in use.

(a) Two devices should not remain connected for more than 23 hours at a time, since the encryption keys can repeat after this.

(b) Encryption should always be enabled for Bluetooth connections. (e.g. "Security Mode 1" does not enable encryption and therefore should never be used.)

CHAPTER 6: POLICY ON PRIVACY CONTROLS

GSA Privacy Controls provide specific guidance on security controls and privacy-related procedures used to protect GSA IT resources. According to NIST, The Privacy Controls are:

- Authority and Purpose (AP)
- Accountability, Audit, and Risk Management (AR)
- Data Quality and Integrity (DI)
- Data Minimization and Retention (DM)
- Individual Participation and Redress (IP)
- Security (SE)
- Transparency (TR)
- Use Limitation (UL)

1. Authority and purpose.

a. **GSA Program officials must consult with the GSA Senior Agency Privacy Officer and/or Privacy Officer (SAOP/PO)** and GSA legal counsel regarding the authority of any program or activity to collect PII.

b. The authority to collect PII is documented in the System of Records Notice (SORN) and/or Privacy Impact Assessment (PIA) or other applicable documentation such as Privacy Act Statements or Computer Matching Agreements.(refer to section 3.12 above for information on Privacy Impact Assessments)

c. Personnel who handle PII must receive training on the organizational authorities for collecting PII, authorized uses of PII, and on the contents of the notice.

2. Accountability, audit, and risk management. The SAOP/PO, in consultation with legal counsel, information security officials, and others as appropriate:

a. Ensures the development, implementation, and enforcement of privacy policies and procedures;

b. Defines roles and responsibilities for protecting PII;

c. Determines the level of information sensitivity with regard to PII holdings;

d. Identifies the laws, regulations, and internal policies that apply to the PII;

e. Monitors privacy best practices; and

f. Monitors/audits compliance with identified privacy controls.

3. Data quality and integrity.

a. GSA programs authorized to collect PII must take reasonable steps to confirm the accuracy and relevance of PII. Such steps may include, editing and validating addresses as they are collected or entered into information systems using automated address verification look-up application programming interfaces (API). The types of measures taken to protect data quality are based on the nature and context of the PII, how it is to be used, and how it was obtained.

b. GSA programs must incorporate mechanisms into information systems and develop corresponding procedures for how frequently, and by what method, the information is to be updated.

4. Data minimization and retention. The GSA SAOP/PO will take appropriate steps to ensure that the collection of PII is consistent with a purpose authorized by law or regulation.

a. The minimum set of PII elements required to support a specific organization business process may be a subset of the PII the organization is authorized to collect.

b. GSA Program officials will consult with the SAOP/PO and legal counsel to identify the minimum PII elements required by the information system or activity to accomplish the legally authorized purpose.

c. GSA will further reduce its privacy and security risks by also reducing its inventory of PII, where appropriate.

5. Individual participation and redress.

a. Depending upon the nature of the program or information system, it may be appropriate to allow individuals to limit the types of PII they provide and subsequent uses of that PII.

b. The GSA information systems may obtain consent through opt-in, opt-out, or implied consent. Opt-in consent is the preferred method, but it is not always feasible. Opt-in requires that individuals take affirmative action to allow organizations to collect or use PII. Opt-out requires individuals to take action to prevent the new or continued collection or use of such PII.

(1) Security. GSA and its agents must take due care in updating PII inventories by identifying linkable data that could create PII. 1. GSA programs may extract the following information elements from Privacy Impact Assessments (PIA) for information systems containing PII: (i) the name and acronym for each system identified; (ii) the types of PII contained in that system; (iii) classification of level of sensitivity of all types of PII, as combined in that information system; and (iv) classification of level of potential risk of substantial harm, embarrassment, inconvenience, or unfairness to affected

individuals, as well as the financial or reputational risks to organizations, if PII is exposed.

(2) Transparency.

(a) GSA must follow the process outlined in the Internal Clearance Process for GSA Data Assets policy before releasing GSA data assets. The established clearance process ensures that the privacy, security and confidentiality of our critical data assets are protected.

(b) At a minimum, GSA programs are required to:

1. Review information for valid restrictions prior to public release in order to ensure proper safeguarding of privacy, security, and confidentiality of Government proprietary and procurement sensitive information;

2. Document reasons why a data asset or certain components of a data asset should not be made public at this time;

3. Consult with the agency's Privacy Officer and general counsel regarding the barriers identified;

4. Encourage dialogue regarding resources necessary to make more data assets public.

(c) GSA programs using PII must provide an Effective Notice, which enables individuals to understand how the GSA organization uses PII generally and, where appropriate, to make an informed decision prior to providing PII to a GSA information system. The Effective notice also demonstrates the privacy considerations that the program or system has addressed in implementing its information practices. GSA may provide a general public notice facilitated through a System of Records Notices (SORNs), Privacy Impact Assessments (PIAs), or in a website privacy policy.

6. Use limitation. The GSA, by way of the SAOP/PO, will ensure the use of PII only for legally authorized purposes and in a manner compatible with uses identified in the Privacy Act and/or in public notices.

a. The PO will perform monitoring and auditing of individual program use of PII

b. Train GSA personnel on the authorized uses of PII

c. With guidance from the SAOP/PO and where appropriate, legal counsel, the GSA programs will document the processes and procedures for evaluating any proposed new uses of PII to assess whether they fall within the scope of the organizational authorities.